

Úvod do teorie množin

Poznámky z předmětu NAIL063 doc. Kynčla

Letní semestr 2023/2024

Jakub Smolík

smolikj@matfyz.cz

Datum poslední změny: 22. října 2025

Obsah

1	Cantorova naivní teorie množin	3
1.1	Russelův paradox	3
1.2	Berryho paradox	3
2	Nejprve trochu logiky	4
2.1	Jazyk teorie množin	4
2.2	Termy a formule	4
3	Axiomy Zermelo-Fraenkelovy teorie množin	5
3.1	Axiom existence	5
3.2	Axiom extenzionality	5
3.3	Axiom dvojice	6
3.4	Axiom sumy	6
3.5	Schéma axiomů vydělení	6
3.6	Axiom potence	7
3.7	Schéma axiomů nahrazení	8
3.8	Axiom fundovanosti	8
3.9	Axiom nekonečna	8
3.10	Axiom výběru a ZFC	9
4	Množiny a třídy	9
4.1	Rozšíření jazyka o třídivé termy	9
4.2	Třídivé operace	10
4.3	Kartézský součin	11
4.4	Relace a zobrazení	11
4.5	Uspořádání	14
4.6	Vlastnosti známých uspořádání	15
4.7	Dedekindovy řezy	16
4.8	Ekvivalence a kvaziuspořádání	16
5	Srovnávání mohutností množin	17
5.1	Cantor-Schröder-Bernsteinova věta	18
5.2	Příklady na srovnávání mohutností množin	20
5.3	Konečné množiny	20
5.3.1	Definice konečnosti	20
5.3.2	Vlastnosti uspořádání konečných množin	21
5.3.3	Operace zachovávající konečnost	24
5.3.4	Princip indukce pro konečné množiny	25
5.4	Přirozená čísla a axiom nekonečna	26
5.4.1	Princip indukce pro přirozená čísla	27
5.4.2	Alternativní definice konečnosti	27
5.4.3	Uspořádání přirozených čísel relací náležitosti	28
5.5	Různě velká nekonečna	30
5.5.1	Spočetné množiny	30
5.5.2	Cantorova věta	31
5.5.3	Kardinalita kontinua	32
5.5.4	Algebraická čísla	33

6	Axiom výběru	33
6.1	Indexované soubory množin	33
6.2	Co axiom výběru tvrdí	34
6.3	Princip maximality	36
6.4	Princip trichotomie	37
6.5	Princip dobrého uspořádání	37
7	Ordinální čísla	38
7.1	Tranzitivní třídy	38
7.2	Uspořádání ordinálních čísel relací náležení	38
7.3	Vlastnosti ordinálních čísel	40
7.4	Typy dobře uspořádaných množin	41
7.5	Princip transfinite indukce	41
7.6	Aplikace konstrukce transfinite rekurzí	43
	Zdroje	44

1 Cantorova naivní teorie množin

Naivní teorii myslíme teorií, která nemá formálně dané axiomy. Místo toho se na její popis používá přirozený jazyk. Na množiny pohlíží jako na soubory libovolných „věcí“. Tento přístup je intuitivní a ve většině případů zcela dostačující. Běžně v matematice pracujeme s množinami tímto způsobem a ničemu to nevadí. Ale ukáže se, že to vede k celé řadě paradoxů.

Sám Cantor si byl například vědom toho, že jeho teorie připouští existenci množiny všech množin, přestože z Cantorovy věty vyplývá, že množina všech množin neexistuje. Tento paradox ale nebyl natolik zásadní, aby donutil Cantora přehodnotit svoji teorii.

Pravděpodobně ten nejdůležitější paradox, který nadobro pohřbil Cantorovu naivní teorii a dal vzniknout axiomatickým teoriím množin, byl Russelův paradox.

1.1 Russelův paradox

Jako první ho zřejmě objevil matematik Ernst Zermelo roku 1899, ale své zjištění nezveřejnil. Publikoval ho až Russell v roce 1901. Návrh první teorie, která se tomuto paradoxu snažila vyhnout, přišel od Zermela v roce 1908. Matematik Abraham Fraenkel ovšem roku 1921 poukázal na to, že v Zermelově teorii není možné dokázat existenci některých množin, jejichž existenci většina tehdejších množinových teoretiků považovala za samozřejmou. Následující rok navrhl úpravu axiomů této teorie, čímž vznikla dnes velmi rozšířená Zermelo-Fraenkelova teorie množin (ZF). Velmi hezké video o Russelově paradoxu je ZDE.

Definice 1.1. Množina M je *krotká* pokud $M \notin M$; jinak je *divoká*.

Například *množina všech zvířat* je krotká, zatímco *množina všech věcí, které nejsou čajové lžičky* je divoká. Zajímavá je třeba *množina všech věcí, na které právě myslím*. Většinou je krotká, ale právě teď, když píšu tuto větu, je divoká.

Podívejme se na množinu všech krotkých množin $M := \{x \mid x \text{ je krotká}\}$. Je krotká, nebo divoká? Pokud je krotká, potom splňuje definiční podmínku M , tedy $M \in M$, takže je divoká. Pokud je divoká, potom nesplňuje definiční podmínku M , tedy $M \notin M$, takže je krotká. Čili je krotká \iff je divoká.

Russelův paradox nám ukazuje, že musíme nějak omezit, co vše může být množinou.

1.2 Berryho paradox

Berryho paradox naopak ukazuje, že definice pomocí přirozeného jazyka mohou vést k paradoxům. Proto se budeme snažit věci definovat jazykem matematické logiky.

Paradox zní následovně: „Označme m nejmenší přirozené číslo, které nelze definovat méně než sto písmeny.“

Anglická abeceda + mezera = 27 znaků, takže celkem 27^{100} kombinací, tedy takovéto m existuje. Víme, že m nelze definovat méně než sto znaky, ale věta výše (která má určitě méně než sto znaků) jej definuje.

2 Nejprve trochu logiky

2.1 Jazyk teorie množin

Jazyk teorie množin je $\langle \in \rangle$ s rovností, kde \in je binární relační symbol. Mohli bychom uvažovat i jazyk bez rovnosti a přidat nový binární relační symbol '=' a axiomy rovnosti. V každém jazyku je implicitně

- spočetně mnoho symbolů pro proměnné: x_1, x_2, x_3, \dots ,
- pro každou proměnnou x dva symboly s kvantifikátory: $(\forall x), (\exists x)$,
- symboly pro logické spojky a pro negaci: $\neg, \wedge, \vee, \implies, \iff$,
- čárka a závorky.

Tento jazyk ještě rozšíříme o několik zkratk. Konkrétně definujeme

- $x \neq y \iff \neg x = y$,
- $x \notin y \iff \neg x \in y$,
- $x \subseteq y \iff (\forall z)(z \in x \implies z \in y)$,
- $x \subset y \iff x \subseteq y \wedge x \neq y$,
- $x \in y \in z \iff x \in y \wedge y \in z$.

2.2 Termy a formule

Nyní uvažujme obecný jazyk L s množinou relačních symbolů \mathcal{R} a množinou funkčních symbolů \mathcal{F} . Konstantní symboly jsou funkční symboly arity nula.

Definice 2.1. *Termy* jazyka L jsou konečné nápisy definované induktivně:

- každá proměnná a každý konstantní symbol z L je term,
- pro funkční symbol f arity n a termy t_1, \dots, t_n je term i nápis $f(t_1, \dots, t_n)$.

Definice 2.2. *Atomická formule* je nápis $R(t_1, \dots, t_n)$, kde R je n -ární relační symbol a t_i jsou termy.

Definice 2.3. *Formule* jazyka L jsou konečné nápisy definované induktivně:

- každá atomická formule jazyka L je formule,
- jsou-li φ a ψ formule, potom jsou formule i nápisy

$$(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \implies \psi), (\varphi \iff \psi), ((\forall x)\varphi), ((\exists x)\varphi).$$

Formule mají přirozenou stromovou strukturu. *Výskyt* proměnné x je list tohoto stromu označený x . *Podformule* jsou podstromy tohoto stromu.

Definice 2.4 (Volné a vázané proměnné). Výskyt proměnné x ve formuli φ je

- *vázaný*, pokud se vyskytuje v nějaké podformuli začínající $(\forall x)$ nebo $(\exists x)$,

- *volný*, pokud není vázaný.

Proměnná x je

- *vázaná* ve formuli φ , pokud má vázaný výskyt ve φ .
- *volná* ve formuli φ , pokud má volný výskyt ve φ .

Úmluva. Zápis $\varphi(x_1, \dots, x_n)$ značí, že x_1, \dots, x_n jsou proměnné, jejichž volné výskyty nás ve formuli φ zajímají. Neznačená to, že každá z proměnných x_i musí mít volný výskyt ve φ , ani že φ neobsahuje žádné jiné volné proměnné.

Příklad. Uvažme formuli $\varphi = (\forall x)(\exists y)(x \leq y) \vee (x \leq z)$. Kvantifikátory se vztahují pouze k první závorce $(x \leq y)$. Proměnná x je vázaná a volná zároveň, y je vázaná a z je volná. Můžeme tedy psát $\varphi(x, z)$.

3 Axiomy Zermelo-Fraenkelovy teorie množin

Až doposud mohly množiny obsahovat libovolné „věci“ a vlastně jsme nijak nespecifikovali, co přesně jsou tyto věci zač. V axiomatické teorii množin existují pouze ty objekty, jejichž existence vyplývá z axiomů dané teorie. Axiomy ZF nám garantují existenci prázdné množiny a poskytují nám několik způsobů jak z již existujících množin vyrábět nové. Jinými slovy: všechno je množina. Každý prvek každé množiny je jen nějaká jiná množina.

3.1 Axiom existence

Axiom 3.1. Existuje nějaká množina, univerzum množin není prázdné.

$$(\exists x)(x = x).$$

3.2 Axiom extenzionality

Axiom 3.2. Množina není dána ničím jiným než svými prvky.

$$(\forall z)(z \in x \Leftrightarrow z \in y) \implies x = y.$$

Je důležité zdůraznit, že toto *není* definice identity dvou množin. Musíme vnímat odděleně dva koncepty. První koncept je naše teorie, ve které můžeme dokazovat různá pravdivá tvrzení. Je to něco zcela abstraktního. Druhý koncept je nějaká konkrétní „implementace“ (model) této teorie. Symbol ‘=’ hovoří o identitě objektů, které poskytne ta konkrétní implementace. My „zevnitř“ naší teorie vůbec netušíme, jak by tato implementace mohla vypadat. Ale máme „zvenčí“ poskytnutý symbol =, který smíme používat. Každá implementace „ví“, co tento symbol znamená. Ale neví, co znamená symbol \in . Axiomy jsou nějaké požadavky, které musí každý model splňovat. Takže tento axiom není definice identity dvou množin, protože identita je koncept, který je odtržený od teorie a přísluší až konkrétnímu modelu. Tento axiom vyjadřuje vztah symbolu \in a identity a každý model bude muset tento požadavek splnit. Opačná implikace,

$$x = y \implies (\forall z)(z \in x \Leftrightarrow z \in y),$$

platí také, ale není součástí axiomu extenzionality, protože vlastně říká, že

$$(\forall z)(z \in x \Leftrightarrow z \in x),$$

což platí pro libovolnou implementaci symbolu \in .

3.3 Axiom dvojice

Axiom 3.3. Pro každou dvojici množin x a y existuje množina d , která obsahuje právě x a y . Množinu d značíme jako $\{x, y\}$.

$$(\forall x, y)(\exists d)(\forall z)(z \in d \Leftrightarrow (z = x \vee z = y)).$$

Tento axiom zaručuje i existenci jednoprvkových množin $\{x\} := \{x, x\}$.

3.4 Axiom sumy

Axiom 3.4. Pro každou množinu x existuje množina s , která je sjednocením všech množin uvnitř x . Této množině říkáme *suma* množiny x a značíme ji $\bigcup x$.

$$(\forall x)(\exists s)(\forall z)(z \in s \Leftrightarrow (\exists y)(y \in x \wedge z \in y)).$$

Pozorování 3.5. Pokud $x \in y \in z$, potom $x \in \bigcup z$.

Nyní můžeme pomocí kombinace axiomu sumy a axiomu dvojice definovat sjednocení dvou množin a libovolně velkou konečnou množinu danou výčtem.

Definice 3.6. Sjednocení množin x a y je množina $x \cup y := \bigcup\{x, y\}$.

Definice 3.7. Množiny $\{x_1\}$ a $\{x_1, x_2\}$ jsou garantované axiomem dvojice. Množinu $\{x_1, x_2, \dots, x_n\}$ definujeme induktivně jako $\{x_1, x_2, \dots, x_{n-1}\} \cup \{x_n\}$.

Příklad. $\bigcup\{\{x_1\}, \{x_1, x_2\}, \{x_2, x_3\}\} = \{x_1, x_2, x_3\}$.

3.5 Schéma axiomů vydělení

Schéma znamená, že se nejedná o jeden konkrétní axiom, ale o nekonečně mnoho různých axiomů, které mají všechny stejnou strukturu.

Axiom 3.8. Pokud je x množina, potom existuje množina všech jejích prvků, které splňují formuli φ . Tuto množinu značíme $\{z \in x \mid \varphi(z)\}$. Formálně, je-li $\varphi(z)$ formule, která neobsahuje volně proměnnou y , potom formule

$$(\forall x)(\exists y)(\forall z)(z \in y \Leftrightarrow (z \in x \wedge \varphi(z))).$$

je axiom.

Všimněme si, že schéma axiomů vydělení nám nedovoluje vyrobit množinu všech množin nebo množinu všech krotkých množin, protože neumožňuje konstrukce typu $\{z \mid \varphi(z)\}$. Použitím axiomu vždy vznikne podmnožina nějaké již existující množiny. Například z množiny X , garantované axiomem existence, lze vyrobit prázdnou množinu tak, že za φ zvolíme libovolnou nesplnitelnou formuli.

Definice 3.9. *Prázdná množina* je množina $\emptyset := \{z \in X \mid z \neq z\}$.

Také konečně můžeme nadefinovat průnik a rozdíl množin.

Definice 3.10. *Rozdíl* množin x a y je množina $x \setminus y := \{z \in x \mid z \notin y\}$.

Definice 3.11. *Průnik* množin x a y je množina $x \cap y := \{z \in x \mid z \in y\}$.

Definice 3.12. Množiny x a y jsou *disjunktní* pokud $x \cap y = \emptyset$.

Definice 3.13. *Průnik* množiny $x \neq \emptyset$ je množina $\bigcap x := \{z \in \bigcup x \mid y \in x \Rightarrow z \in y\}$.

Příklad. Průnik konečně mnoha množin x_1, x_2, \dots, x_n lze zapsat dvěma způsoby:

$$\bigcap \{x_1, x_2, \dots, x_n\} = x_1 \cap x_2 \cap \dots \cap x_n.$$

Průnik nekonečně mnoha množin už ovšem lze udělat pouze jako průnik nekonečné množiny x .

Poznámka. Důvod, proč zatím nedefinujeme průnik prázdné množiny je ten, že s touto definicí bychom měli $\bigcap \emptyset = \emptyset$, což moc nedává smysl. Prázdný součet je nula, prázdný součin je jedna a prázdná suma je prázdná množina. Vše to jsou neutrální prvky vůči dané operaci. Co je neutrální prvek vůči průniku? Prázdná množina určitě ne. Nabízí se množina všech množin, ale ukážeme, že ta neexistuje. Tento problém vyřešíme v sekci 4.2.

Definice 3.14. *Uspořádaná dvojice* (a, b) je množina $\{\{a\}, \{a, b\}\}$. Uspořádanou n -tici (a_1, a_2, \dots, a_n) potom definujeme induktivně jako $((a_1, a_2, \dots, a_{n-1}), a_n)$.

Lemma 3.15. *Uspořádaná dvojice určuje své prvky jednoznačně. Tedy*

$$(x, y) = (a, b) \iff (x = a \wedge y = b).$$

Důkaz. Nejprve ' \Leftarrow '. Z axiomu extenzionality máme $\{x\} = \{a\}$ a $\{x, y\} = \{a, b\}$ a tedy i $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$. Nyní ' \Rightarrow '. Ukážeme, že (a, b) jednoznačně určuje pořadí svých prvků. Označme $P := \bigcap(a, b)$ a $S := \bigcup(a, b)$. Potom platí

$$\{a\} = P, \quad \{b\} = \{z \in S \mid z \neq a \vee P = S\}. \quad \square$$

3.6 Axiom potence

Axiom 3.16. Pro každou množinu x existuje množina všech jejích podmnožin. Této množině říkáme *potenční množina* množiny x a značíme ji $\mathcal{P}(x)$.

$$(\forall x)(\exists p)(\forall z)(z \in p \iff z \subseteq x).$$

Pozorování 3.17. *Potenční množina a suma jsou svým způsobem opačné operace:*

$$z \subseteq x \Rightarrow z \in \mathcal{P}(x), \quad z \in x \Rightarrow z \subseteq \bigcup x, \quad \bigcup \mathcal{P}(x) = x \subseteq \mathcal{P}(\bigcup x)$$

3.7 Schéma axiomů nahrazení

Axiom 3.18. Když si vezmeme libovolné zobrazení F a množinu vzorů A , tak množina obrazů $B = F[A]$ je také množina. Formálně, je-li $\psi(x,y)$ formule, která neobsahuje volně proměnné y_1, y_2 a b , potom formule

$$(\forall x)(\forall y_1, y_2)((\psi(x, y_1) \wedge \psi(x, y_2)) \Rightarrow y_1 = y_2) \Rightarrow \\ (\forall a)(\exists b) : (\forall y)(y \in b \Leftrightarrow (\exists x)(x \in a \wedge \psi(x, y)))$$

je axiom. Formule $\psi(x, y_1)$, resp. $\psi(x, y_2)$ vzniknou z formule $\psi(x, y)$ substitucí proměnné y_1 , resp. y_2 za y .

První část tohoto axiomu říká, že $\psi(x, y)$ se má chovat jako zobrazení $y = F(x)$. Ve druhé polovině značí a množinu vzorů a b množinu obrazů, které těmto vzorům odpovídají.

Pozorování 3.19. Pokud za $\psi(x, y)$ zvolíme formuli $x = y \wedge \varphi(y)$, tak je první část axiomu nahrazení splněna. Tedy platí, že

$$(\forall a)(\exists b)(\forall y)(y \in b \Leftrightarrow (\exists x)(x \in a \wedge x = y \wedge \varphi(y))),$$

což je jen trochu jinak zapsaný axiom vydělení.

3.8 Axiom fundovanosti

Axiom 3.20. Každá neprázdná množina obsahuje nějakou množinu, která je s ní disjunktní.

$$(\forall x \neq \emptyset)(\exists y \in x)(x \cap y = \emptyset).$$

Důsledek 3.21. Neexistuje množina a splňující $a \in a$.

Důkaz. Pro spor nechť a je divoká. Potom množina $\{a\}$ nesplňuje fundovanost, protože $a \in a$ a zároveň $a \in \{a\}$, takže $a \in a \cap \{a\}$. \square

Důsledek 3.22. Neexistuje dvojice množin a, b taková, že $a \in b$ a $b \in a$. Tentokrát poruší fundovanost množina $\{a, b\}$.

Tento axiom nám zaručuje, že v ZF nemůže vzniknout Russelův paradox, protože vylučuje možnost existence divokých a dalších divných množin. Také z něj vyplývá, že v ZF neexistuje množina všech množin, protože ta by určitě byla divoká.

3.9 Axiom nekonečna

Axiom 3.23. Existuje nekonečná množina s nějakou konkrétní strukturou.

$$(\exists w)(\emptyset \in w \wedge (\forall z)(z \in w \Rightarrow z \cup \{z\} \in w)).$$

Axiom nekonečna nám umožní definovat množinu všech přirozených čísel, jako nejmenší množinu splňující tuto podmínku.

3.10 Axiom výběru a ZFC

Axiom výběru, anglicky Axiom of choice (AC), je natolik silné tvrzení, že není součástí základní verze Zermelo-Fraenkelovy teorie. Jeho přidáním do ZF získáme mnohem silnější teorii ZFC. Bez něj nelze dokázat mnoho věcí, které by intuitivně měly platit, ale některé jeho důsledky jsou na hranici paradoxnosti, proto byl historicky velmi kontroverzní. Budeme se jím zabývat ve zvláštní kapitole.

4 Množiny a třídy

Dokázali jsme, že v ZF množina všech množin neexistuje. Ale chtěli bychom, aby existovalo něco podobného, protože občas chceme mluvit o souboru všech objektů, které něco splňují, přestože to už není množina. Proto se zavádí pojem *třída*. V Cantorově naivní teorii jsou třídy a množiny jedno a totéž. Pokud omezíme, co všechno může být množinou, tak se náš svět rozdělí.

- Množiny — někam náleží.
- Třídy — něco náleží do nich.

Uvědomme si, že tento koncept neumožňuje zrekonstruovat Russellův paradox, jelikož třída všech krotkých tříd zjevně neexistuje. Třídy totiž nemohou nikam náležet, věci pouze náleží do nich.

4.1 Rozšíření jazyka o třídivé termy

Třída je pouze meta-jazykový pojem, v ZF nejsou formálně definované.

Definice 4.1 (Třída). Pokud je $\varphi(x)$ formule, potom výraz $\{x \mid \varphi(x)\}$ nazýváme *třídivý term*. Definuje „soubor“ všech množin x , pro které platí $\varphi(x)$. Tomuto souboru říkáme *třída* určená formulí $\varphi(x)$.

Pozorování 4.2. Pokud je $\varphi(x)$ ve tvaru $x \in y \wedge \psi(x)$, kde y je množina, tak třída $\{x \mid \varphi(x)\}$ je množina (z axiomu vydělení).

Pozorování 4.3. Každá množina je zároveň i třídou, protože $x = \{z \mid z \in x\}$.

Definice 4.4. Třidu, která není množinou, nazýváme *vlastní třída*.

Ve formulích na místě volných proměnných připustíme třídivé termy. Navíc dovolíme třídivé proměnné, které budeme značit velkými písmeny. Ale pouze jako volné proměnné, takže třídy není možné kvantifikovat.

Definice 4.5 (Formule s třídivými termy). Atomické formule v tomto rozšířeném jazyce jsou

$$x = y, \quad x \in y, \quad x = X, \quad x \in X, \quad X \in x, \quad X = Y, \quad X \in Y,$$

kde x, y jsou proměnné, X je zkratka za $\{z \mid \varphi(z)\}$ a Y za $\{z \mid \psi(z)\}$.

Každá atomická formule je formule a libovolná kombinace formulí pomocí logických spojek je opět formule. Množinové proměnné lze navíc kvantifikovat.

Tvrzení 4.6. Pro každou formuli s třídovými termy, ale bez třídových proměnných, existuje ekvivalentní formule v základním jazyce.

Důkaz. Eliminujeme třídové termy. Mějme množiny x, y, z , logické formule $\varphi(x)$ a $\psi(y)$ a třídové termy $X = \{x \mid \varphi(x)\}$ a $Y = \{y \mid \psi(y)\}$. Přepíšeme všechny atomické formule do základního jazyka.

- $z \in X \sim z \in \{x \mid \varphi(x)\} \sim \varphi(z)$,
- $X = Y \sim \{x \mid \varphi(x)\} = \{y \mid \psi(y)\} \sim (\forall u)(\varphi(u) \Leftrightarrow \psi(u))$.

Dále budeme využívat, že X nemůže být vlastní třída.

- $z = X \sim z = \{x \mid \varphi(x)\} \sim (\forall u)(u \in z \Leftrightarrow \varphi(u))$,
- $X \in Y \sim \{x \mid \varphi(x)\} \in \{y \mid \psi(y)\} \sim (\exists u)(u = \{x \mid \varphi(x)\} \wedge u \in \{y \mid \psi(y)\}) \sim (\exists u)((\forall v)(v \in u \Leftrightarrow \varphi(v)) \wedge \psi(u))$,
- $X \in y \sim \{x \mid \varphi(x)\} \in y \sim (\exists u)(u = \{x \mid \varphi(x)\} \wedge u \in y) \sim (\exists u)((\forall v)(v \in u \Leftrightarrow \varphi(v)) \wedge u \in y)$. □

Důsledek 4.7. Formule rozšířeného jazyka určují stejné třídy jako formule základního jazyka. Třídové termy slouží pouze pro usnadnění zápisu.

Formule s třídovými proměnnými lze interpretovat jako schémata formulí základního jazyka. Za třídovou proměnnou totiž můžeme dosadit jakýkoli třídový term, který odpovídá nějaké formuli základního jazyka.

4.2 Třídové operace

Definice 4.8. Pro třídy A a B definujeme

- $A \cap B := \{x \mid x \in A \wedge x \in B\}$,
- $A \cup B := \{x \mid x \in A \vee x \in B\}$,
- $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$, ... případně $A - B$
- $\bigcup A := \{x \mid (\exists a)(a \in A \wedge x \in a)\}$,
- $\bigcap A := \{x \mid (\forall a)(a \in A \Rightarrow x \in a)\}$
- $A \subseteq B \iff (\forall x)(x \in A \Rightarrow x \in B)$, ... A je podtřídou B
- $A \subset B \iff A \subseteq B \wedge A \neq B$, ... A je vlastní podtřídou B
- $\mathcal{P}(A) := \{x \mid x \subseteq A\}$.

Pozorování 4.9. Průnik prázdné množiny je třída všech množin.

Definice 4.10 (Univerzální třída). Třidu všech množin $V := \{x \mid x = x\}$ nazýváme *univerzální třída*. Třidu $V \setminus A$ nazýváme *absolutní doplněk* třídy A .

Pozorování 4.11. Platí $\mathcal{P}(V) = V$.

Důkaz. Necht' x je libovolná množina. Ukážeme, že $x \in \mathcal{P}(V)$. Platí to, protože $(\forall z)(z \in x \Rightarrow z \in V)$, tedy $x \subseteq V$, z čehož $x \in \mathcal{P}(V)$. □

Lemma 4.12. Je-li a množina a $A = \{x \mid \varphi(x)\}$ třída, potom je $a \cap A$ množina.

Důkaz. Z axiomu vydělení máme $a \cap A = \{x \in a \mid \varphi(x)\}$. □

4.3 Kartézský součin

Definice 4.13. *Kartézský součin tříd A a B je třída*

$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}.$$

Kartézský součin tříd A_1, A_2, \dots, A_n definujeme induktivně jako

$$A_1 \times \dots \times A_n := (A_1 \times \dots \times A_{n-1}) \times A_n = \{(a_1, \dots, a_n) \mid \bigwedge_{i=1}^n a_i \in A_i\}.$$

Lemma 4.14. *Jsou-li x a y množiny, potom je $x \times y$ také množina.*

Důkaz. Idea těchto důkazů: najít nějakou hodně velkou množinu a pak použít axiom vydělení. Dokážeme, že platí

$$x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y)).$$

Uspořádanou dvojici jsme definovali jako $(a, b) = \{\{a\}, \{a, b\}\}$. Pokud $a \in x$ a $b \in y$, tak $\{a\}, \{a, b\} \subseteq x \cup y$ neboli $\{a\}, \{a, b\} \in \mathcal{P}(x \cup y)$. Tedy $(a, b) \subseteq \mathcal{P}(x \cup y)$, z čehož $(a, b) \in \mathcal{P}(\mathcal{P}(x \cup y))$. \square

Definice 4.15 (Kartézská mocnina). Pro třídu X definujeme $X^1 := X$ a pak induktivně $X^n := X^{n-1} \times X = \prod_{i=1}^n X$.

Pozorování 4.16. *Pro univerzální třídu platí $V = V^1 \supseteq V^2 \supseteq V^3 \supseteq \dots$.*

Důkaz. Každá n -tice je i dvojice (tak je definována), ale lze ji dokonce vnímat jako k -tici pro libovolné $k \leq n$. Například jako trojici $(a, b, c) = ((a, b), c)$:

$$(x_1, \dots, x_{n-1}, x_n) = ((x_1, \dots, x_{n-1}), x_n) = (((x_1, \dots, x_{n-2}), x_{n-1}), x_n). \quad \square$$

Příklad. Definujeme $X^3 := X^2 \times X$, ale $X \times X^2 \neq X^3$. Mají stejnou strukturu, ale v teorii množin to jsou různé objekty. Zvolme třeba $X = \{\emptyset\}$. Máme

- $X^2 \times X = \{(\emptyset, \emptyset)\} \times \{\emptyset\} = \{((\emptyset, \emptyset), \emptyset)\},$
- $X \times X^2 = \{\emptyset\} \times \{(\emptyset, \emptyset)\} = \{(\emptyset, (\emptyset, \emptyset))\}.$

4.4 Relace a zobrazení

Definice 4.17. Rozšíříme náš jazyk o další zkratky. Nechť A je třída a φ formule.

- $(\exists x \in A)(\varphi) \iff (\exists x)(x \in A \wedge \varphi),$
- $(\nexists x \in A)(\varphi) \iff (\forall x)(x \notin A \vee \neg \varphi),$
- $(\forall x \in A)(\varphi) \iff (\forall x)(x \in A \Rightarrow \varphi).$

Poslední zkratku definujeme pouze pro formule $\varphi(x)$ bez volných výskytů y a z :

- $(\exists! x \in A)(\varphi) \iff (\exists x \in A)(\varphi) \wedge (\forall y \in A)(\forall z \in A)((\varphi(y) \wedge \varphi(z)) \Rightarrow y = z).$

Definice 4.18. *Binární relace* je libovolná třída $R \subseteq V \times V$. Namísto $(x, y) \in R$ píšeme $x R y$. Podobně lze definovat n -ární relaci jako $R \subseteq V^n$.

Definice 4.19. Pro (binární) relaci R a třídu X definujeme třídy

- $R^{-1} := \{(v,u) \mid u R v\}$, ... *inverzní relace* k relaci R
- $\text{Dom}(R) := \{u \mid (\exists v)(u R v)\}$, ... *definiční obor* relace R
- $\text{Rng}(R) := \{v \mid (\exists u)(u R v)\}$, ... *obor hodnot* relace R
- $R \upharpoonright X := R \cap (X \times V) \subseteq R$, ... *zúžení relace* R na třídu X
- $R[X] := \text{Rng}(R \upharpoonright X) \subseteq \text{Rng}(R)$ *obraz třídy* X relací R

Pozorování 4.20. $R \subseteq \text{Dom}(R) \times \text{Rng}(R)$, $R^{-1} \subseteq \text{Rng}(R) \times \text{Dom}(R)$.

Lemma 4.21. *Pokud je relace x množina a Y třída, potom x^{-1} , $\text{Dom}(x)$, $\text{Rng}(x)$, ale i $x \upharpoonright Y$ a $x[Y]$ jsou také množiny.*

Důkaz. Pomocí axiomu vydělení.

- Ukážeme $\text{Dom}(x) \subseteq \bigcup(\bigcup x)$. Pro libovolné $u \in \text{Dom}(x)$ existuje v t.ž. $(u,v) \in x$. Máme posloupnost inkluzí $u \in \{u\} \in (u,v) \in x$, tedy $u \in \bigcup(\bigcup x)$.
- Podobně $\text{Rng}(x) \subseteq \bigcup(\bigcup x)$, zkrátka to $v \in \text{Rng}(x)$ je třeba vybalit z té uspořádané dvojice $(u,v) \in x$ jako $v \in \{u,v\} \in (u,v) \in x$.
- $x^{-1} \subseteq \text{Rng}(x) \times \text{Dom}(x)$... kartézský součin množin je množina.
- $x[Y] \subseteq \text{Rng}(x)$ a $x \upharpoonright Y \subseteq x$. □

Definice 4.22. Relace odpovídající relačním symbolům jazyka teorie množin jsou

- $E := \{(x,y) \mid x \in y\}$, ... *náležení*
- $\text{Id} := \{(x,y) \mid x = y\}$ *identita*
- $\Delta_X := \text{Id} \upharpoonright X$... *identita na třídě* X

Definice 4.23 (Skládání relací). Pro relace R a S definujeme relaci

$$R \circ S := \{(u,w) \mid (\exists v)(u R v \wedge v S w)\}$$

Příklad. $\text{Id} \circ R = R \circ \text{Id} = R$, $(x,y) \in E \circ E \iff x \in \bigcup y$.

Definice 4.24 (Zobrazení). Relace F je *zobrazení* (nebo *funkce*) pokud

$$(\forall u)(\forall v)(\forall w)((u,v) \in F \wedge (u,w) \in F \Rightarrow v = w).$$

Namísto $u F v$ píšeme $F(u) = v$, při definování píšeme $F : u \mapsto v$.

Pozorování 4.25. F je *zobrazení* $\iff (\forall x \in \text{Dom}(F))(\exists! y \in \text{Rng}(F))(F(x) = y)$.

Definice 4.26 (Prosté zobrazení, bijekce). Řekneme, že zobrazení F je

- *prosté*, pokud je F^{-1} také zobrazení,
- zobrazení třídy X do třídy Y pokud $\text{Dom}(F) = X \wedge \text{Rng}(F) \subseteq Y$, píšeme $F : X \rightarrow Y$,

- zobrazení třídy X na třídu Y , pokud $F : X \rightarrow Y \wedge \text{Rng}(F) = Y$,
- *bijekce* mezi třídami X a Y , pokud je to prosté zobrazení X na Y .

Pozorování 4.27. *Pokud je F prosté, potom je F^{-1} také prosté.*

Lemma 4.28. *Pokud je f zobrazení a $\text{Dom}(f)$ množina, potom f je také množina.*

Důkaz. Axiom nahrazení nám říká, že zobrazení zobrazují množiny na množiny, tedy $f[\text{Dom}(f)] = \text{Rng}(f)$ je množina a z axiomu vydělení je tedy $f \subseteq \text{Dom}(f) \times \text{Rng}(f)$ také množina. \square

Definice 4.29 (Třída zobrazení mezi množinami). Pro třídu A a množinu a definujeme třídu všech zobrazení z množiny a do třídy A jako

$${}^a A := \{f \mid f : a \rightarrow A\}.$$

Poznámka. Nelze definovat ${}^B A$ pokud B je vlastní třída, potom by ta zobrazení $f : B \rightarrow A$ už byla vlastní třídy. Obměnou f je množina $\Rightarrow \text{Dom}(f)$ je množina.

Pozorování 4.30. *Tohle ještě nemáme pořádně definované, ale pokud jsou A a B konečné množiny, potom $|{}^B A| = |A|^{|B|}$.*

Příklad. ${}^\emptyset A = \{\emptyset\}$ a ${}^a \emptyset = \emptyset$, ovšem ${}^\emptyset \emptyset = \{\emptyset\}$. $\dots 0^0 := 1$.

Lemma 4.31 (O velikosti třídy zobrazení). *Platí následující.*

1. Pro libovolné množiny x, y je ${}^x y$ množina.
2. Je-li $x \neq \emptyset$ a Y vlastní třída, potom je ${}^x Y$ vlastní třída.

Důkaz. První část pomocí axiomu vydělení, druhá pomocí nahrazení.

1. $f : x \rightarrow y$, pak $f \subseteq x \times y$, tedy $f \in \mathcal{P}(x \times y)$, takže ${}^x y \subseteq \mathcal{P}(x \times y)$. Využíváme, že kartézský součin množin je množina.
2. Pro každé $y \in Y$ definujeme konstantní zobrazení $K_y : x \rightarrow Y$ jako $u \mapsto y$, neboli $K_y = x \times \{y\}$. Protože $x \neq \emptyset$, tak pro $y_1 \neq y_2$ je $K_{y_1} \neq K_{y_2}$. Označme $K := \{K_y \mid y \in Y\}$. Zřejmě $K \subseteq {}^x Y$. Sporem ukážeme, že K je vlastní třída, (takže ${}^x Y$ taky). Předpokládejme, že K je množina a definujme zobrazení $F : K \rightarrow Y, K_y \mapsto y$. Protože předpokládáme, že K je množina, tak z axiomu nahrazení je i Y množina, ale to je spor. \square

Definice 4.32 (Vlastnosti relací). Nechť $R \subseteq V \times V$ je relace a X třída. Označme $R_X := R \upharpoonright X$. Řekneme, že relace R je na třídě X

- *reflexivní*, pokud $\Delta_X \subseteq R$,
- *antireflexivní*, pokud $\Delta_X \cap R = \emptyset$,
- *symetrická*, pokud $R_X = R_X^{-1}$,
- *slabě antisymetrická*, pokud $R_X \cap R_X^{-1} \subseteq \Delta_X$,
- *silně antisymetrická*, pokud $R_X \cap R_X^{-1} = \emptyset$,
- *tranzitivní*, pokud $R_X \circ R_X \subseteq R_X$.

Pozorování 4.33. *Tyto vlastnosti jsou dědičné, neboli platí na každé podtřídě $Y \subseteq X$.*

4.5 Uspořádání

Definice 4.34 (Uspořádání). Relace $R \subseteq V \times V$ je na třídě X

- *trichotomická*, pokud $(\forall x, y \in X)(x R y \vee y R x \vee x = y)$,
- *ostré uspořádání* pokud je antireflexivní a tranzitivní na X ,
- *uspořádání* pokud je reflexivní, slabě antisymetrická a tranzitivní na X ,
- *lineární uspořádání* pokud je trichotomická a uspořádání na X .

Pokud je R uspořádání, tak místo $x R y$ píšeme $x \leq_R y$. Dále definujeme ostré uspořádání $R' := R \setminus \text{Id}$. Namísto $x R' y$ píšeme $x <_R y$.

Poznámka. Jelikož lze z ostrého uspořádání $<_R$ snadno vyrobit \leq_R a naopak, tak nebudeme definovat vlastnosti zvlášť pro ostré a neostré uspořádání, jelikož jedno implicitně definuje to druhé. Ve větách a důkazech budeme používat tu verzi uspořádání, která se nám zrovna bude hodit víc.

Pozorování 4.35. Každé ostré uspořádání R je silně antisymetrické.

Důkaz. Kdyby ne, tak existují $x, y \in X$ t.ž. $x R y$ a $y R x$. Z tranzitivity $x R x$, což je spor s antireflexibilitou. \square

Příklad. Identita není ostré uspořádání, protože není antireflexivní. Identita je uspořádání. Ale ne lineární, protože různé prvky nejsou porovnatelné. Nálezení není uspořádání (ani ostré uspořádání), protože není tranzitivní.

Definice 4.36. Nechť R je uspořádání na třídě A a $X \subseteq A$. Prvek $a \in A$ je

- *horní mez* třídy X , pokud $(\forall x \in X)(x \leq_R a)$, ... také *majoranta*
- *maximální prvek* třídy X , pokud $a \in X \wedge (\nexists x \in X)(a <_R x)$,
- *největší prvek* třídy X , pokud $a \in X$ a je to horní mez X ,
- *supremum* třídy X , pokud je nejmenší prvek třídy všech horní mezí X .

Největší prvek, resp. supremum značíme $\max_R(X)$, resp. $\sup_R(X)$; pokud existují. Obdobně definujeme *minorantu*, *minimální prvek*, *nejmenší prvek* a *infimum*.

Pozorování 4.37. Každý největší prvek je maximální. Pokud je R lineární uspořádání, tak maximální prvek je nejvýše jeden a pokud existuje, tak je největší. Největší prvek i supremum je vždy nejvýše jedno.

Definice 4.38 (Dolní množina). Nechť R je uspořádání na třídě A . Třída $X \subseteq A$ je

- *shora omezená* v A , pokud existuje $a \in A$ horní mez X ,
- *dolní množina* v A , pokud $(\forall x \in X)(\forall a \in A)(a \leq_R x \Rightarrow a \in X)$.

Každý prvek $a \in A$ určuje dolní množinu

$$(\leftarrow, a] := \{x \mid x \in A \wedge x \leq_R a\}.$$

Pozorování 4.39. *Sjednocení dolních množin je dolní množina.*

Pozorování 4.40. *Nechť R je uspořádání na třídě A . Pak pro libovolné $x, y \in A$ platí*

$$x \leq_R y \iff (\leftarrow, x] \subseteq (\leftarrow, y].$$

Čili uspořádání \subseteq na $\mathcal{P}(A)$ je svým způsobem univerzální. Každé uspořádání lze převést na inkluzi.

Definice 4.41. Řekneme, že uspořádání R je na množině A

- *husté*, pokud $(\forall x, y \in A)(x < y \Rightarrow (\exists z \in A)(x < z < y))$,
- *dobré*, pokud každá neprázdná $B \subseteq A$ má nejmenší prvek,
- *úplné*, pokud každá neprázdná, shora omezená $B \subseteq A$ má supremum.

Pokud je \leq lineární, resp. dobré uspořádání množiny A , tak říkáme, že (A, \leq) je *lineárně*, resp. *dobře uspořádaná množina*. Pokud existuje nějaké úplné uspořádání množiny A , tak říkáme, že A je *úplná*.

Pozorování 4.42. *Linearity, dobrá a úplnost jsou dědičné vlastnosti.*

Pozorování 4.43. *Každé dobré uspořádání je lineární. Kdyby nebylo, tak by existovaly nějaké dva neporovnatelné prvky a množina těchto dvou prvků by neměla nejmenší prvek.*

4.6 Vlastnosti známých uspořádání

Níže je uvedeno několik známých uspořádání a jejich vlastnosti.

- (\mathbb{N}, \leq) Přirozená čísla se standardní interpretací \leq je dobře uspořádaná množina. Její nejmenší prvek je nula.
- (\mathbb{Z}, \leq) Standardní uspořádání celých čísel je lineární, ale není dobré, protože vůči \leq neexistuje nejmenší celé číslo.
- (\mathbb{Z}, \preceq) Uspořádání $x \preceq y \iff (|x| < |y|) \vee (|x| = |y| \wedge x \leq y)$ celých čísel je dobré. Toto uspořádání vypadá následovně: $0, -1, 1, -2, 2, -3, 3, \dots$
- (\mathbb{Q}, \leq) Standardní uspořádání racionálních čísel je lineární a husté, ale není dobré, protože \mathbb{Q} nemá žádný nejmenší prvek vůči \leq . Ovšem není těžké sestavit nějaké dobré uspořádání. Racionální čísla nejsou úplná.
- (\mathbb{R}, \leq) Standardní uspořádání reálných čísel je lineární, husté a úplné. Ale není dobré a dokonce ani nevíme, jestli v ZF nějaké dobré uspořádání reálných čísel vůbec existuje.
- $(\mathbb{N}^+, |)$ Přirozená čísla bez nuly spolu s relací dělitelnosti jsou částečné uspořádání. Toto uspořádání nemá žádný maximální prvek, ale zato má nejmenší prvek, a sice jedničku.
- $(\mathcal{P}(A), \subseteq)$ Potenční množina libovolné množiny A spolu s inkluzí je částečně uspořádaná množina. V tomto uspořádání je prázdná množina \emptyset nejmenší prvek a A největší prvek.
- (Σ^*, \leq_{LEX}) Lexikografické uspořádání konečných řetězců nad abecedou Σ je dobré uspořádání. Nejmenší prvek je prázdný řetězec.

4.7 Dedekindovy řezy

Níže předvedeme jednu z možných konstrukcí \mathbb{R} z \mathbb{Q} , konkrétně pomocí takzvaných dedekindových řezů. Předpokládejme, že \mathbb{Q} už máme.

Definice 4.44. Množina $X \subseteq \mathbb{Q}$ je *dedekindův řez*, pokud

1. X je dolní množina \mathbb{Q} ,
2. existuje-li $\sup_{\mathbb{Q}}(X)$, potom $\sup_{\mathbb{Q}}(X) \in X$.

Takže třeba $\mathbb{Q} \cap (-\infty, 1)$ není dedekindův řez, ale $\mathbb{Q} \cap (-\infty, 1]$ ano. Jinak by to nebylo jednoznačné. Ovšem $\mathbb{Q} \cap (-\infty, \sqrt{2}) = \mathbb{Q} \cap (-\infty, \sqrt{2}]$ je dedekindův řez, protože tato množina nemá v \mathbb{Q} supremum.

Definice 4.45. Reálná čísla definujeme jako $\mathbb{R} := \{x \in \mathcal{P}(\mathbb{Q}) \mid x \text{ je dedekindův řez}\}$.

My s reálnými čísly ovšem většinou budeme pracovat spíše jako s nekonečnými binárními zápisy.

4.8 Ekvivalence a kvaziuspořádání

Definice 4.46. Relace $R \subseteq V \times V$ je na třídě X

- *kvaziuspořádání* pokud je reflexivní a tranzitivní na X ,
- *ekvivalence* pokud je reflexivní, symetrická a tranzitivní na X .

Definice 4.47 (Třídy ekvivalence). Nechť R je ekvivalence na třídě X . Pro $x \in X$ definujeme třídu

$$[x]_R := \{y \mid y \in X \wedge x R y\} = R[\{x\}] \cap X,$$

kterou nazýváme *ekvivalenční třída* prvku x . Pokud je X množina, tak z axiomu vydělení je $[x]_R$ také množina. V tom případě definujeme *množinu ekvivalenčních tříd* množiny X podle ekvivalence R jako

$$X/R := \{[x]_R \in \mathcal{P}(X) \mid x \in X\}.$$

Definice 4.48. *Rozklad množiny X* je libovolná množina $\mathcal{R} \subseteq \mathcal{P}(X)$ splňující

1. $(\forall a \in \mathcal{R})(a \neq \emptyset)$,
2. $(\forall a, b \in \mathcal{R})(a \neq b \Rightarrow a \cap b = \emptyset)$,
3. $\bigcup \mathcal{R} = X$.

Lemma 4.49. *Pokud je \sim ekvivalence na množině X , potom je X/\sim rozklad X .*

Důkaz. Musíme ukázat, že X/\sim splňuje definici rozkladu.

1. Z reflexivity $x \sim x$, tedy $x \in [x]$ pro každé $[x] \in X/\sim$.
2. Obměnou: ukážeme $[x] \cap [y] \neq \emptyset \Rightarrow [x] = [y]$. Chceme ukázat, že pokud existuje $t \in [x] \cap [y]$ a $a \in [x]$, potom $a \in [y]$. Víme, že $a \sim x$, $x \sim t$, $t \sim y$ a tudíž z tranzitivity $a \sim y$. Použili jsme i symetrii.

3. Stačí ukázat, že pokud $x \in X$, potom existuje $a \in X/\sim$ t.ž. $x \in a$. Ale toto a je prostě $[x]$. \square

Pozorování 4.50. Pokud je relace \lesssim kvaziuspořádání na množině X , potom můžeme definovat ekvivalenci \sim na X předpisem

$$x \sim y \iff x \lesssim y \wedge y \lesssim x.$$

Potom můžeme definovat uspořádání \leq na množině X/\sim jako

$$[x]_{\sim} \leq [y]_{\sim} \iff x \lesssim y.$$

Tato konstrukce je velmi šikovná, často se totiž potýkáme s množinou X , která je skoro uspořádaná relací R , až na to, že R není antisymetrická na některých podmnožinách X . Potom prostě prohlásíme tyto zlobivé prvky za ekvivalentní a definujeme nové uspořádání na třídách ekvivalence.

Ovšem pokud je X vlastní třída, tak to nemusí fungovat. Může se stát, že pro nějaké $x \in X$ bude $[x]_{\sim}$ také vlastní třída, a potom nelze definovat X/\sim .

5 Srovnávání mohutností množin

Definice 5.1. Pro množiny x a y definujeme relace

1. $x \approx y$, pokud existuje bijekce $f : x \rightarrow y$,
2. $x \preceq y$, pokud existuje prosté zobrazení $f : x \rightarrow y$,
3. $x \prec y$, pokud $x \preceq y$ a $x \not\approx y$.

Poznámka. Pro třídy tato definice nemá smysl, protože je nelze kvantifikovat.

Poznámka. Relaci $x \preceq y$ jsme také mohli definovat jako „existuje zobrazení y na x “. Ale potom by Věta 5.7 nešla dokázat bez AC. Důvod je následující.

Platí: Existuje-li prosté zobrazení x do y , potom existuje zobrazení y na x . Prostě vezmu ten jednoznačně určený prvek. Ale opačný směr bez AC neplatí, protože se na jeden prvek může zobrazit až nekonečně mnoho prvků a tohle se může stát nekonečně-mnoho krát, takže to prosté zobrazení v opačném směru bez AC nesestrojím.

Pozorování 5.2. Pro libovolné množiny x, y, z platí

- $x \subseteq y \implies x \preceq y$,
- $x \subset y \implies x \preceq y$, ... ale ne $x \prec y$
- $x \approx x$, ... identitou
- $x \approx y \implies y \approx x$, ... inverzní bijekcí
- $(x \approx y \wedge y \approx z) \implies x \approx z$, ... složení bijekcí je bijekce
- $x \preceq x$, ... identitou
- $(x \preceq y \wedge y \preceq z) \implies x \preceq z$, ... složení prostých zobr. je prosté

- \preceq je trichotomická \iff platí axiom výběru.

Důsledek 5.3. *Relace \approx je ekvivalence a \preceq je kvaziuspořádání. Ale ne uspořádání, protipříklad na antisymetrii je třeba $\{\emptyset\}$ a $\{\{\emptyset\}\}$.*

Příklad. Mohli bychom z kvaziuspořádání \preceq vyrobit uspořádání na ekvivalenčních třídách $[x]_{\approx}$? Bohužel ne, protože to jsou vlastní třídy, takže V/\approx neexistuje. Kdyby pro nějaké $x \neq \emptyset$ byla $[x]_{\approx}$ množina, tak $V = \bigcup [x]_{\approx}$ by také byla množina.

Lemma 5.4. *Nechť x, y, x_1, y_1 a z jsou množiny. Pak*

1. $x \times y \approx y \times x$,
2. $x \times (y \times z) \approx (x \times y) \times z$,
3. $(x \approx x_1 \wedge y \approx y_1) \implies (x \times y) \approx (x_1 \times y_1)$,
4. $x \approx y \implies \mathcal{P}(x) \approx \mathcal{P}(y)$,
5. $\mathcal{P}(x) \approx {}^x 2$. $\dots 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$

Důkaz. Vždy sestrojíme nějakou bijekci h .

1. $h : (u, v) \mapsto (v, u)$,
2. $h : (a, (b, c)) \mapsto ((a, b), c)$,
3. $f : x \rightarrow x_1$ a $g : y \rightarrow y_1$. Uděláme $h : (a, b) \mapsto (f(a), g(b))$,
4. $f : x \rightarrow y$. Uděláme $h : u \mapsto f[u]$,
5. Pro $u \subseteq x$ definujeme charakteristickou funkci $\chi_u : x \rightarrow \{0, 1\}$ předpisem

$$\chi_u(a) := \begin{cases} 1, & a \in u, \\ 0, & a \notin u. \end{cases}$$

Bijekci $h : \mathcal{P}(x) \rightarrow {}^x 2$ definujeme jako $h : u \mapsto \chi_u$. □

5.1 Cantor-Schröder-Bernsteinova věta

Definice 5.5 (Monotónní zobrazení). Zobrazení $H : \mathcal{P}(x) \rightarrow \mathcal{P}(y)$ je *monotónní vzhledem k inkluzi*, pokud pro všechny $u, v \subseteq x$ platí

$$u \subseteq v \implies H(u) \subseteq H(v).$$

Příklad. $A \subseteq \mathcal{P}(x)$ uspořádaná pomocí \subseteq , pak $\sup_{\subseteq}(A) = \bigcup A$ a $\inf_{\subseteq}(A) = \bigcap A$.

Lemma 5.6 (O pevném bodu). *Je-li $H : \mathcal{P}(x) \rightarrow \mathcal{P}(x)$ monotónní vzhledem k inkluzi, pak existuje $c \in \mathcal{P}(x)$ takové, že $H(c) = c$.*

Intuice. Představme si na chvíli, že H je funkce reálných čísel a chceme najít její pevný bod. Potom dává smysl se podívat na množinu $\{x \mid x \leq H(x)\}$. Nemělo by nás překvapit, kdyby supremum této množiny byl pevný bod.

Důkaz. Necht $A := \{u \in \mathcal{P}(x) \mid u \subseteq H(u)\}$ a označme $c := \sup_{\subseteq}(A) = \bigcup A$. Ukážeme, že $H(c) = c$. Pro každou $u \in A$ platí

$$\begin{array}{ll} u \subseteq c, & c \text{ je horní mez } A \\ u \subseteq H(u), & u \in A \\ H(u) \subseteq H(c), & H \text{ je monotónní} \\ u \subseteq H(c). & \text{z předchozích dvou} \end{array} \quad (5.1)$$

Tedy $H(c)$ je horní mez A . Protože c je nejmenší horní mez A , tak platí

$$\begin{array}{ll} c \subseteq H(c), & c \text{ je supremum } A \\ H(c) \subseteq H(H(c)), & H \text{ je monotónní} \\ H(c) \in A, & \text{podle 5.2} \\ H(c) \subseteq c. & \text{podle 5.1} \end{array} \quad (5.2)$$

Máme inkluzi v obou směrech, takže $c = H(c)$. □

Věta 5.7 (Cantor, Schröder, Bernstein). $x \approx y \iff (x \preceq y \wedge y \preceq x)$.

Důkaz. Směr ‘ \Rightarrow ’ je triviální. Pro ‘ \Leftarrow ’ necht $f : x \rightarrow y$ a $g : y \rightarrow x$ jsou prostá zobrazení. Uvažme „indukovaná“ zobrazení

$$\begin{array}{ll} \mathbf{f} : \mathcal{P}(x) \rightarrow \mathcal{P}(y) & \mathbf{g} : \mathcal{P}(y) \rightarrow \mathcal{P}(x) \\ u \mapsto f[u], & v \mapsto g[v]. \end{array}$$

Například $\mathbf{f}(\{1, 2, 3\}) = \{f(1), f(2), f(3)\}$. Všimněme si, že \mathbf{f} i \mathbf{g} jsou monotónní vzhledem k inkluzi. Chceme zobrazit kus x pomocí \mathbf{f} na kus y a zbytek y zobrazit pomocí \mathbf{g} zpátky na zbytek x . Ale obecně to nemusí dohromady vyplnit celou množinu x a můžou tam být nějaké duplicity.

Definujme zobrazení $H : \mathcal{P}(x) \rightarrow \mathcal{P}(x)$ jako $H : u \mapsto x - \mathbf{g}(y - \mathbf{f}(u))$. Dělá to, co je popsáno výše a na konci vezme doplněk. Naším cílem je najít nějaké $c \subseteq x$, aby $H(c) = c$, tedy c a $\mathbf{g}(y - \mathbf{f}(c))$ tvoří rozklad x . Stačí ukázat, že H je monotónní vzhledem k inkluzi. Vezměme libovolné $u \subseteq v \subseteq x$. Máme

$$\begin{array}{ll} \mathbf{f}(u) \subseteq \mathbf{f}(v), & \mathbf{f} \text{ je monotónní} \\ y - \mathbf{f}(u) \supseteq y - \mathbf{f}(v), & \text{doplněk do } y \\ \mathbf{g}(y - \mathbf{f}(u)) \supseteq \mathbf{g}(y - \mathbf{f}(v)), & \mathbf{g} \text{ je monotónní} \\ H(u) \subseteq H(v). & \text{doplněk do } x \end{array}$$

Podle Lemmatu 5.6 má H pevný bod, označme jej c . Tedy $c = x - \mathbf{g}(y - \mathbf{f}(c))$, takže $g[y - \mathbf{f}(c)] = x - c$. To znamená, že restrikce $g \upharpoonright (y - \mathbf{f}(c))$ je prosté zobrazení $y - \mathbf{f}(c)$ na $x - c$, čili bijekce. Inverze bijekce je opět bijekce, tedy $g^{-1} \upharpoonright (x - c)$ je bijekce mezi $x - c$ a $y - \mathbf{f}(c)$. To doplníme bijekcí $f \upharpoonright c$ mezi c a $f[c]$, čímž získáme bijekci $h := (f \upharpoonright c) \cup (g^{-1} \upharpoonright (x - c))$, jinými slovy

$$h(a) = \begin{cases} f(a), & a \in c, \\ g^{-1}(a), & a \in x - c, \end{cases}$$

mezi x a y a můžeme prohlásit, že $x \approx y$. □

5.2 Příklady na srovnávání mohutností množin

Množinu přirozených čísel danou axiomem nekonečna budeme značit ω . Ovšem pokud budeme chtít o přirozených číslech mluvit jako o *číslech* a ne jako o *množinách*, tak budeme stále používat značení \mathbb{N} .

Příklad. $\omega \approx \omega \times \omega$. Využijeme Větu 5.7 a definujeme prostá zobrazení

$$\begin{aligned} f : \omega &\rightarrow \omega \times \omega & g : \omega \times \omega &\rightarrow \omega \\ n &\mapsto (n, 0), & (a, b) &\mapsto 2^a \cdot 3^b. \end{aligned}$$

Zobrazení g je prosté ze základní věty aritmetiky.

Příklad. $\omega \approx \mathbb{Q}$. Zlomky jsou vlastně uspořádané trojice $\mathbb{Q} \subseteq \omega \times \omega \times 2$. Například $-3/4 \sim (3, 4, 1)$ nebo $4/8 \sim (4, 8, 0)$. Definujeme prostá zobrazení

$$\begin{aligned} f : \omega &\rightarrow \mathbb{Q} & g : \mathbb{Q} &\rightarrow \omega \\ n &\mapsto (n, 1, 0), & (a, b, s) &\mapsto 2^a \cdot 3^b \cdot 5^s. \end{aligned}$$

Čili $\omega \preceq \mathbb{Q}$ a zároveň $\mathbb{Q} \preceq \omega$, tedy podle Cantor-Bernsteinovy věty $\omega \approx \mathbb{Q}$.

Příklad. $[0, 1]^2 \approx [0, 1]$, tedy čtverec se zobrazí na úsečku. Hezké vysvětlení je ZDE.

Lemma 5.8. *Pokud pro množinu x platí $x \times x \approx x$, tak $x^n \approx x$ pro každé $n \in \mathbb{N}$.*

Důkaz. Když $n = 1$, tak hledaná bijekce je identita. Předpoklad nám dává bijekci $f_2 : x^2 \rightarrow x$, pomocí které induktivně definujeme bijekce $f_{n+1} : x^{n+1} \rightarrow x$ jako

$$f_{n+1} : (a_1, \dots, a_{n+1}) \mapsto f_2(f_n(a_1, \dots, a_n), a_{n+1}). \quad \square$$

5.3 Konečné množiny

5.3.1 Definice konečnosti

Nejpřirozenější definice je: x je konečná, pokud $(\exists n \in \omega)(x \approx n)$. My to uděláme trochu oklikou, protože s touto definicí se špatně dokazují tvrzení.

Definice 5.9 (Tarski). Množina x je *konečná*, pokud každá neprázdná $a \subseteq \mathcal{P}(x)$ má maximální prvek vůči inkluzi. Pokud je x konečná, tak píšeme $\text{Fin}(x)$.

Intuice. Tohle zjevně platí pro všechny konečné množiny. Vyberu nějaký prvek. Pokud je maximální, vyhrál jsem. Pokud není, tak existuje větší, vyberu jej a opakuji. Ale třeba pro množinu přirozených čísel \mathbb{N} to už neplatí. Když označíme $[n] := \{1, 2, \dots, n\}$, tak množina $\{[n] \mid n \in \mathbb{N}\} \subseteq \mathcal{P}(\mathbb{N})$ nemá maximální prvek. Všimněme si, že podobný protipříklad můžeme zkonstruovat pro libovolnou nekonečnou množinu.

Pozorování 5.10. *Množina x je konečná \iff každá neprázdná $a \subseteq \mathcal{P}(x)$ má minimální prvek vůči inkluzi.*

Důkaz. Definujeme $d : \mathcal{P}(x) \rightarrow \mathcal{P}(x)$, $u \mapsto x \setminus u$. Potom $u \subseteq v \iff d(u) \supseteq d(v)$. Klíčová úvaha: v je maximum množiny $a \subseteq \mathcal{P}(x) \iff d(v)$ je minimum množiny $d[a] = \{d(u) \mid u \in a\}$. \square

Lemma 5.11. *Je-li x konečná a y nekonečná, potom $x \prec y$.*

Důkaz. Pro spor necht $y \preceq x$, tedy existuje prosté zobrazení $f : y \rightarrow x$. Jelikož y je nekonečná, tak existuje $\emptyset \neq u \subseteq \mathcal{P}(y)$, která nemá maximální prvek vůči inkluzi. Definujme zobrazení $g : \mathcal{P}(y) \rightarrow \mathcal{P}(x)$ jako $g : a \mapsto f[a]$. Nyní množinu $u \subseteq \mathcal{P}(y)$ zobrazíme na množinu $g[u] \subseteq \mathcal{P}(x)$. Protože je x konečná, tak $g[u]$ má maximální prvek vůči inkluzi, označme jej m . Zobrazme nyní m pomocí g^{-1} zpátky do u , čímž získáme $n_0 := g^{-1}(m) \in u$. Jelikož u nemá maximální prvek vůči inkluzi, tak existuje $n_1 \in u$ t.ž. $n_0 \subset n_1$. Jelikož je f prostá, tak jsou g a g^{-1} také prosté, a proto $m = g(n_0) \subset g(n_1)$, což je spor s maximalitou m . \square

Definice 5.12. Množina x je *dedekindovsky konečná*, pokud $(\forall y)(y \subset x \Rightarrow y \prec x)$.

Lemma 5.13. *Je-li x konečná, potom je i dedekindovsky konečná.*

Důkaz. Pro spor necht pro nějaké $y \subset x$ platí $y \approx x$ a definujeme množinu všech takových zlobivých y jako

$$A := \{y \subset x \mid y \approx x\}.$$

Protože $A \neq \emptyset$ a $A \subseteq \mathcal{P}(x)$, tak z konečnosti x existuje c , minimální prvek A vůči inkluzi. Protože $x \approx c$, tak existuje bijekce $f : x \rightarrow c$. Označme $d := f[c]$. Protože $c \subset x$, tak $f[c] \subset f[x]$, tedy $d \subset c$. Jenže $f \upharpoonright c$ je bijekce mezi c a d , tedy $c \approx d$, z čehož $d \approx x$, tedy $d \in A$. To je spor s minimalitou c . \square

Poznámka. Opačná implikace nelze dokázat v ZF, potřebujeme AC. V ZF dokonce existují dedekindovsky konečné množiny x , pro které je $\mathcal{P}(x)$ dedekindovsky nekonečná. Proto ta definice není moc šikovná.

Poznámka. Další ekvivalentní definice konečnosti s Tarského. $\text{Fin}(x) \iff$

- existuje lineární uspořádání ' \leq ' na x , které je dobré, a ' \geq ' je také dobré.
- existuje lineární uspořádání na x a každá dvě lin. usp. jsou izomorfní.
- $\mathcal{P}(\mathcal{P}(x))$ je dedekindovsky konečná.
- $(\exists n \in \omega)(x \approx n)$.

5.3.2 Vlastnosti uspořádání konečných množin

Lemma 5.14. *Je-li a konečná množina, uspořádaná relací \leq , potom má každá neprázdná $b \subseteq a$ minimální i maximální prvek vůči \leq .*

Důkaz. Maximalitu vůči \leq převedeme na maximalitu vůči \subseteq . Máme (a, \leq) a $\emptyset \neq b \subseteq a$. Pro každé $x \in b$ uvažme $(\leftarrow, x] \subseteq a$. Označme $u := \{(\leftarrow, x] \mid x \in b\} \subseteq \mathcal{P}(a)$. Jelikož $u \neq \emptyset$ a a je konečná, tak u má minimální i maximální prvek vůči inkluzi. Všimněme si, že pokud je $(\leftarrow, m]$ maximální v u vzhledem k \subseteq , tak m je maximální v b vzhledem k \leq . Obdobně pro minimum. \square

Věta 5.15. *Každé lineární uspořádání na konečné množině je dobré.*

Důkaz. Je to přímý důsledek: v lineárním uspořádání je minimální prvek automaticky i nejmenší. \square

Definice 5.16 (Izomorfismus). Necht' A_1, A_2 jsou třídy a R_1, R_2 relace. Bijekce $F : A_1 \rightarrow A_2$ je *izomorfismus* tříd A_1, A_2 vzhledem k relacím R_1, R_2 , pokud

$$(\forall x, y \in A_1)((x, y) \in R_1 \iff (F(x), F(y)) \in R_2).$$

Příklad. Speciálním případem izomorfismu je izomorfismus grafů. Tam jsou třídy A_1 a A_2 množiny vrcholů grafů G_1 a G_2 , relace R_1 je relací „být hranou v G_1 “ a R_2 je relací „být hranou v G_2 “. Potom je bijekce $f : V_1 \rightarrow V_2$ izomorfismus grafů $G_1 = (V_1, E_1)$ a $G_2 = (V_2, E_2)$ právě tehdy, když

$$(\forall u, v \in V_1)((u, v) \in E_1 \iff (f(u), f(v)) \in E_2).$$

Izomorfismy se hodí i když hovoříme o uspořádáních. Řekneme, že F je počátkové vnoření A do B , je-li to izomorfismus nějakých dolních podmnožin A a B .

Definice 5.17 (Počátkové vnoření). Necht' (A, \leq_R) a (B, \leq_S) jsou uspořádané množiny. Zobrazení F je *počátkové vnoření* A do B , pokud

1. $A_D := \text{Dom}(F) \subseteq A$ je dolní množina v A vůči \leq_R ,
2. $B_D := \text{Rng}(F) \subseteq B$ je dolní množina v B vůči \leq_S .
3. F je izomorfismus A_D a B_D , vzhledem k R a S , tedy

$$(\forall a_1, a_2 \in A_D)(a_1 \leq_R a_2 \iff F(a_1) \leq_S F(a_2)),$$

Lemma 5.18. Necht' F a G jsou počátková vnoření dobře uspořádané množiny (A, \leq_R) do dobře uspořádané množiny (B, \leq_S) . Pak platí, že $F \subseteq G$ nebo $G \subseteq F$.

Důkaz. Jelikož $\text{Dom}(F)$ i $\text{Dom}(G)$ jsou dolní množiny A a R je lineární, tak buď $\text{Dom}(F) \subseteq \text{Dom}(G)$, nebo naopak. BÚNO necht' $\text{Dom}(F) \subseteq \text{Dom}(G)$. Zřejmě $F, G \subseteq A \times B$, takže stačí dokázat, že

$$x \in \text{Dom}(F) \implies F(x) = G(x).$$

Pro spor necht' to neplatí a definujme

$$W := \{x \in \text{Dom}(F) \mid F(x) \neq G(x)\}.$$

Protože R je dobré, tak existuje $w := \min_R(W)$. Jelikož $F(w) \neq G(w)$, tak z linearity S nastane buď $F(w) <_S G(w)$ nebo $G(w) <_S F(w)$, BÚNO necht' platí

$$F(w) <_S G(w). \tag{5.3}$$

Ukážeme, že $F(w) \notin \text{Rng}(G)$, takže $\text{Rng}(G)$ není dolní množina B , což je spor. Pro libovolné $z \in \text{Dom}(G)$ nastane jedna ze dvou situací:

1. $z <_R w$, z čehož $G(z) <_S F(w)$, protože

$$\begin{array}{ll} G(z) = F(z), & w \text{ je nejmenší, pro který se nerovnají} \\ F(z) <_S F(w). & F \text{ je izomorfismus} \end{array}$$

2. $w \leq_R z$, z čehož $F(w) <_S G(z)$, protože

$$\begin{aligned} F(w) &<_S G(w), & \text{podle (5.3)} \\ G(w) &\leq_S G(z). & G \text{ je izomorfismus} \end{aligned}$$

V každém případě $F(w) \neq G(z)$, tedy $F(w) \notin \text{Rng}(G)$. \square

Věta 5.19 (O porovnávání dobrých uspořádání). *Pokud jsou (A, \leq_R) a (B, \leq_S) dobře uspořádané množiny, tak existuje právě jedno zobrazení F , které je izomorfismem A a nějaké dolní podmnožiny B , nebo izomorfismem B a nějaké dolní podmnožiny A . Tedy minimálně jedna z těchto množin se celá vyčerpá a F je počátkové vnoření.*

Důkaz. Označme P množinu všech počátkových vnoření A do B . Tvrdíme, že $F := \bigcup P$ je ten hledaný izomorfismus. Ověříme všechny podmínky:

1. F je zobrazení. Když $(x, y_1), (x, y_2) \in F$, tak existují počátková vnoření $F_1, F_2 \in P$ t.ž. $(x, y_1) \in F_1$ a $(x, y_2) \in F_2$. Podle Lemmatu 5.18 platí $F_1 \subseteq F_2$ nebo $F_2 \subseteq F_1$. V každém případě jsou obě ty dvojice v alespoň jednom z F_1 nebo F_2 , ale protože to jsou zobrazení, tak musí být $y_1 = y_2$.
2. F je prosté. Podobně, jenom využijeme, že F_1 a F_2 jsou počátková vnoření, tedy izomorfismy, tedy bijekce, takže jsou prosté, z čehož $x_1 = x_2$.
3. F je počátkové vnoření
 - (a) $\text{Dom}(F)$ je dolní množina v A . Necht' $x \in \text{Dom}(F)$, $y \in A$ a $y <_R x$. Potřebujeme ukázat, že $y \in \text{Dom}(F)$. Jelikož $x \in \text{Dom}(F)$, tak existuje nějaké počátkové vnoření $F' \in P$ t.ž. $x \in \text{Dom}(F')$. Protože $\text{Dom}(F')$ je dolní množina, tak $y \in \text{Dom}(F') \subseteq \text{Dom}(F)$.
 - (b) $\text{Rng}(F)$ je dolní množina v B . Úplně stejná argumentace.
 - (c) F je izomorfismus. Nejprve si uvědomme, že protože je F prosté, tak je to bijekce mezi množinami $\text{Dom}(F)$ a $\text{Rng}(F)$. Nyní necht' $x, y \in \text{Dom}(F)$, potřebujeme aby

$$x \leq_R y \iff F(x) \leq_S F(y).$$

Opět musí existovat nějaké $F' \in P$ t.ž. $y \in \text{Dom}(F')$. F' je počátkové vnoření, takže $\text{Dom}(F')$ je dolní množina, tedy $x \in \text{Dom}(F')$. Navíc, protože je F' izomorfismus, tak

$$F(x) = F'(x) \leq_S F'(y) = F(y).$$

4. $\text{Dom}(F) = A$ nebo $\text{Rng}(F) = B$. Pro spor necht' $A \setminus \text{Dom}(F)$ i $B \setminus \text{Rng}(F)$ jsou neprázdné. Tedy mají nejmenší prvky a, b . Všimněme si, že $F' := F \cup \{(a, b)\}$ je také počátkové vnoření, tedy $F' \in P$, což je spor. Proč je to počátkové vnoření? Protože $\text{Dom}(F)$ je dolní množina v A , tak všechny prvky v $A \setminus \text{Dom}(F)$ musí být větší než všechno v $\text{Dom}(F)$. Tedy a bude nový největší prvek v $\text{Dom}(F')$. Podobně pro b a izomorfismus.

5. Jednoznačnost. Pro spor nechť existují dvě taková zobrazení $F_1 \neq F_2$. Podle Lemmatu 5.18 nechť BÚNO $F_1 \subseteq F_2$. Protože $F_1 \neq F_2$, tak existuje nějaké $(a, b) \in F_2 \setminus F_1$. Jenže potom pro F_1 nemůže platit 4, což je spor. \square

Věta 5.20. *Každá dvě lineární uspořádání na konečné množině jsou izomorfní.*

Důkaz. Nechť R, S jsou lineární uspořádání na konečné množině x . Protože x je konečná, tak díky Větě 5.15 jsou to dokonce dobrá uspořádání. Máme tedy dvě dobře uspořádané množiny, (x, \leq_R) a (x, \leq_S) . Podle předchozí věty je množina (x, \leq_R) izomorfní s nějakou dolní množinou (a, \leq_S) , kde $a \subseteq x$. Mohlo by to být i naopak, ale BÚNO uvažme tuto variantu. Chceme ukázat, že $x = a$. Pro spor nechť $a \subset x$. Jelikož se jedná o izomorfismus, tedy speciálně bijekci, tak $a \approx x$. Což ale znamená, že x není dedekindovsky konečná, a to je spor s Lemmatem 5.13. \square

5.3.3 Operace zachovávající konečnost

Lemma 5.21. *Platí*

1. $\text{Fin}(x) \wedge y \subseteq x \implies \text{Fin}(y)$,
2. $\text{Fin}(x) \wedge y \approx x \implies \text{Fin}(y)$,
3. $\text{Fin}(x) \wedge y \preceq x \implies \text{Fin}(y)$.

Důkaz. 1. Ukážeme, že libovolná $\emptyset \neq w \subseteq \mathcal{P}(y)$ má maximální prvek. To je jednoduché, protože $w \subseteq \mathcal{P}(y) \subseteq \mathcal{P}(x)$, tudíž $w \subseteq \mathcal{P}(x)$ a x je konečná.
 2. Zřejmě $\mathcal{P}(x) \approx \mathcal{P}(y)$, dokonce jsou izomorfní vzhledem k \subseteq . Vynecháme detaily.
 3. Plyne z předchozích dvou. Vezmeme nějakou $z \subseteq x$ takovou, že $z \approx y$. \square

Lemma 5.22. *Sjednocení konečných množin je konečné:*

1. $\text{Fin}(x) \wedge \text{Fin}(y) \implies \text{Fin}(x \cup y)$,
2. $\text{Fin}(x) \implies (\forall y) \text{Fin}(x \cup \{y\})$ triviální důsledek 1

Důkaz. Nechť $\emptyset \neq w \subseteq \mathcal{P}(x \cup y)$, nalezneme maximální prvek. Idea je taková, že se zvlášť podíváme na x -ové a y -ové prvky množin ve w , najdeme maxima a zkombinujeme je. Definujme zobrazení

$$\begin{array}{ll} f_x : w \rightarrow \mathcal{P}(x) & f_y : w \rightarrow \mathcal{P}(y) \\ u \mapsto u \cap x, & u \mapsto u \cap y. \end{array}$$

Potom označme

$$w_x := \{f_x(u) \mid u \in w\}.$$

Zřejmě $\emptyset \neq w_x \subseteq \mathcal{P}(x)$, takže má maximální prvek vůči inkluzi, označme jej v_x . Nyní položíme

$$w_y := \{f_y(u) \mid u \in w \wedge f_x(u) = v_x\}.$$

Opět $\emptyset \neq w_y \subseteq \mathcal{P}(y)$, takže má maximální prvek v_y . Všimněme si, že $v_x \cup v_y$ je hledaný maximální prvek množiny w . Kdyby ne, tak by to byl spor s maximalitou v_x nebo v_y . \square

5.3.4 Princip indukce pro konečné množiny

Definice 5.23. Definujeme třídu všech konečných množin $\text{Fin} := \{x \mid \text{Fin}(x)\}$

Věta 5.24 (princip indukce pro konečné množiny). *Je-li X třída, pro kterou platí*

1. $\emptyset \in X$,
2. $x \in X \Rightarrow (\forall y)(x \cup \{y\} \in X)$,

potom $\text{Fin} \subseteq X$.

Důkaz. Pro spor nechť existuje nějaká množina $x \in \text{Fin} \setminus X$. Definujeme

$$w := \{v \subseteq x \mid v \in X\}.$$

Podle 1 je $\emptyset \in w$, takže $\emptyset \neq w \subseteq \mathcal{P}(x)$. Protože je x konečná, tak w má maximální prvek vůči inkluzi, označme jej v_0 . Tedy $v_0 \subseteq x$, ale $v_0 \neq x$, protože $v_0 \in X$. To znamená, že existuje nějaký prvek $y \in x \setminus v_0$. Položme $v_1 := v_0 \cup \{y\}$. Podle 2 platí $v_1 \in w$, což je spor s maximalitou v_0 . \square

Lemma 5.25. $\text{Fin}(x) \implies \text{Fin}(\mathcal{P}(x))$.

Důkaz. Pomocí principu indukce. Ukážeme, že třída $X := \{x \mid \text{Fin}(\mathcal{P}(x))\}$ splňuje obě dvě podmínky, z čehož $\text{Fin} \subseteq X$ a platí to pro všechny konečné množiny.

1. $\emptyset \in X$, protože $\mathcal{P}(\emptyset) = \{\emptyset\}$ je konečná množina.
2. Nechť $x \in X$ a y je libovolná množina, ukážeme $x \cup \{y\} \in X$. BÚNO $y \notin x$. Rozdělíme $\mathcal{P}(x \cup \{y\})$ na dvě části: $\mathcal{P}(x)$ a $z := \mathcal{P}(x \cup \{y\}) \setminus \mathcal{P}(x)$. Všimněme si, že $\mathcal{P}(x) \approx z$ bijekcí $f : \mathcal{P}(x) \rightarrow z, u \mapsto u \cup \{y\}$. Z předpokladu je $\mathcal{P}(x)$ konečná, tedy z konečná také a sjednocení konečných množin je konečné, tedy $\mathcal{P}(x) \cup z = \mathcal{P}(x \cup \{y\})$ je konečná množina. \square

Důsledek 5.26. $\text{Fin}(x) \wedge \text{Fin}(y) \implies \text{Fin}(x \times y)$

Důkaz. $x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y))$, jak jsme již ukázali v důkazu Lemma 4.14. \square

Lemma 5.27. *Sjednocení konečně mnoha konečných množin je konečná množina.*

$$\text{Fin}(x) \wedge (\forall a \in x) \text{Fin}(a) \implies \text{Fin}\left(\bigcup x\right).$$

Důkaz. Pomocí principu indukce. Nechť $X = \{x \mid x \subseteq \text{Fin} \Rightarrow \text{Fin}(\bigcup x)\}$.

1. $\emptyset \in X$, protože $\bigcup \emptyset = \emptyset$ a $\text{Fin}(\emptyset)$.
2. Nechť $x \in X$, y je libovolná množina, ukážeme $x \cup \{y\} \in X$. Pokud y je nekonečná, tak $x \cup \{y\} \not\subseteq \text{Fin}$. Jinak její suma je

$$\bigcup (x \cup \{y\}) = y \cup \bigcup x.$$

Na pravé straně je sjednocení dvou konečných množin, což je konečná množina. \square

Důsledek 5.28 (Dirichletův princip pro nekonečné množiny). *Je-li nekonečná množina sjednocením konečně mnoha množin, pak alespoň jedna z nich je nekonečná.*

V úvodu do této kapitoly jsme zmiňovali, že v ZF nelze dokázat, že relace \preceq je trichotomická. Ovšem pro konečné množiny to lze pomocí indukce.

Lemma 5.29. *Každá konečná množina je srovnatelná se všemi množinami.*

$$\text{Fin}(x) \implies (\forall y)(x \preceq y \vee y \preceq x).$$

Důkaz. Indukcí. Položme $X := \{x \mid (\forall y)(x \preceq y \vee y \preceq x)\}$.

1. $\emptyset \in X$ protože $(\forall y) : \emptyset \subseteq y$, takže $\emptyset \preceq y$.
2. Nechť $x \in X$, u je libovolná množina a $z = x \cup \{u\}$. Chceme ukázat, že $z \in X$. BÚNO $u \notin x$. Nechť y je libovolná množina. Podle předpokladu je $x \preceq y$ nebo $y \preceq x$. Mohou nastat dvě možnosti:

- (a) $y \preceq x$, pak $y \preceq x \cup \{u\}$.
- (b) $x \prec y$, ukážeme $x \cup \{u\} \preceq y$. Nechť $f : x \mapsto y$ je prosté zobrazení x do y . Jelikož $x \prec y$, tak existuje $v \in y \setminus f[x]$. Definujme $g : x \cup \{u\} \rightarrow y$ jako $g := f \cup (u, v)$. g je prosté zobrazení $x \cup \{u\}$ do y , tedy $x \cup \{u\} \preceq y$. \square

Úloha. Pokud $\text{Fin}(x)$ a $f : x \rightarrow y$, potom $\text{Rng}(f) \preceq x$.

Úloha. Každou konečnou množinu lze dobře uspořádat.

5.4 Přirozená čísla a axiom nekonečna

Zermelo chtěl přirozená čísla definovat jako $0 := \emptyset$ a $n := \{n - 1\}$. Russel a Frege zase jako $n := \{x \mid x \text{ má } n \text{ prvků}\}$, to jsou ale vlastní třídy. Dnes se používá definice, kterou navrhl Von Neumann:

$$0 := \emptyset, 1 := \{0\}, 2 := \{0, 1\}, \dots, n + 1 := \{0, 1, \dots, n\} = n \cup \{n\}.$$

Definice 5.30. Definujeme funkci následníka jako $S : V \rightarrow V$, $v \mapsto v \cup \{v\}$.

Definice 5.31. Množina w je *induktivní*, pokud $\emptyset \in w \wedge (\forall v \in w)(S(v) \in w)$. Píšeme $\text{Ind}(w)$.

Axiom 5.32 (Nekonečna). Existuje nějaká induktivní množina, neboli $(\exists x) \text{Ind}(x)$.

Definice 5.33. Množina všech přirozených čísel je $\omega := \bigcap \{w \mid \text{Ind}(w)\}$.

Lemma 5.34. ω je nejmenší induktivní množina.

Důkaz. Pokud je w induktivní, tak $\emptyset \in w$, takže $\emptyset \in \omega$. Pokud $n \in \omega$, tak $(\forall w)(\text{Ind}(w) \Rightarrow n \in w)$, tedy i $S(n) \in w$ a tudíž $S(n) \in \omega$. \square

5.4.1 Princip indukce pro přirozená čísla

Věta 5.35. *Pokud $X \subseteq \omega$ a X je induktivní, potom $X = \omega$.*

Důkaz. Z definice ω platí $\omega \subseteq X$, tedy máme inkluzi v obou směrech. \square

Důsledek 5.36. *Chceme dokázat $(\forall n \in \omega) \varphi(n)$, místo toho dokážeme*

$$\varphi(0) \quad \wedge \quad (\forall n \in \omega)(\varphi(n) \Rightarrow \varphi(S(n))).$$

Potom podle principu indukce platí $X := \{x \in \omega \mid \varphi(x)\} = \omega$.

Lemma 5.37 (o vlastnostech přirozených čísel). *Pro libovolná $n, m \in \omega$ platí*

1. $n \in \omega \Rightarrow n \subseteq \omega$,
2. $m \in n \Rightarrow m \subseteq n$,
3. $n \notin n$.

Důkaz.

1. Dokážeme indukcí podle n . Pro nulu to platí, protože $0 \subseteq \omega$. Potom pro $n \in \omega$ už máme $n \subseteq \omega$. Protože $n \in \omega$, tak $\{n\} \subseteq \omega$ a i $n \cup \{n\} \subseteq \omega$
2. Indukcí podle n . Pro nulu to zjevně platí. Nyní nechť to platí pro n . Chceme ukázat, že pokud $m \in S(n)$, potom $m \subseteq S(n)$. Jelikož $m \in S(n) = n \cup \{n\}$, tak buď $m \in n$ a podle i.p. $m \subseteq n \subseteq S(n)$. Nebo $m = n \subseteq S(n)$.
3. Pro nulu to platí. Nyní nechť $n \in \omega$ a $n \notin n$. Pro spor předpokládejme, že $S(n) \in S(n) = n \cup \{n\}$. Potom buď $S(n) \in n$ nebo $S(n) = n$. V obou případech dostáváme inkluzi $S(n) \subseteq n$. Jenomže $S(n) = n \cup \{n\}$, takže $n \in n$ což je spor s i.p. \square

5.4.2 Alternativní definice konečnosti

Lemma 5.38. *Každé přirozené číslo je konečná množina. Neboli $n \in \omega \Rightarrow \text{Fin}(n)$.*

Důkaz. Indukcí. Zjevně $\text{Fin}(0)$. Nyní nechť pro $n \in \omega$ platí $\text{Fin}(n)$. Podle lemmatu o sjednocování konečných množin máme $\text{Fin}(n \cup \{n\})$ \square

Věta 5.39. *Množina x je konečná $\iff (\exists n \in \omega)(x \approx n)$.*

Důkaz. Směr ' \Leftarrow ' z lemmatu. Opačný směr indukcí pro konečné množiny. Definujeme množinu

$$X := \{x \mid (\exists n \in \omega)(x \approx n)\}.$$

Splníme předpoklady principu indukce, z čehož poplyne $\text{Fin}(x) \Rightarrow x \in X$.

1. $\emptyset \in X$, protože $\emptyset \approx 0$.
2. Nechť $x \in X$ a y je množina. Chceme ukázat $x \cup \{y\} \in X$. Máme $x \approx n$ pro nějaké $n \in \omega$. BÚNO nechť $y \notin x$ (jinak $x \cup \{y\} = x \approx n$). Tvrdíme, že $x \cup \{y\} \approx S(n)$. Bijekci $f : x \rightarrow n$ rozšíříme o prvek (y, n) , čímž získáme bijekci $g : x \cup \{y\} \rightarrow S(n)$. Tedy $x \cup \{y\} \approx S(n)$ a $x \cup \{y\} \in X$. \square

Lemma 5.40. ω je nekonečná. ... všechny ostatní induktivní množiny také

Důkaz. Musíme najít nějakou neprázdnou podmnožinu $\mathcal{P}(\omega)$, která nemá maximální prvek. Ukáže se, že to je samotná ω . Podle lemmatu o vlastnostech přirozených čísel pro každé $n \in \omega$ platí $n \subseteq \omega$, tedy $n \in \mathcal{P}(\omega)$, proto $\omega \subseteq \mathcal{P}(\omega)$. Zjevně $\omega \neq \emptyset$. Ukážeme, že nemá maximální prvek vůči inkluzi. Když $n \in \omega$, tak $n \subset n \cup \{n\} \in \omega$, tedy n není maximální. \square

Lemma 5.41. ω je dedekindovsky nekonečná.

Důkaz. Musíme najít nějakou množinu $w \subset \omega$ takovou, že $w \approx \omega$. Vezmeme množinu $w := \omega \setminus \{0\}$. Naší bijekcí je funkce následníka $S : \omega \rightarrow w$. \square

Poznámka. Jelikož každá konečná množina je ded. konečná, tak každý ded. nekonečná množina je nekonečná (obměna). Což je další důkaz nekonečnosti ω .

5.4.3 Uspořádání přirozených čísel relací náležení

Lemma 5.42. Pro libovolná $n, m \in \omega$ platí

$$m \in n \iff m \subset n$$

Důkaz. Směr ' \Rightarrow ' plyne z $m \subseteq n$ a $n \notin n$. Směr ' \Leftarrow ' indukci podle n . Pro $n = 0$ nelze splnit předpoklad $m \subset 0$, takže to platí. Nyní necht' to platí pro nějaké $n \in \omega$. Předpokládáme, že $m \subset S(n)$, budeme chtít ukázat, že $m \in S(n)$.

Ukážeme $m \subseteq n$, tedy buď $m \subset n$ a podle i.p. $m \in n$, nebo $m = n$, každopádně $m \in n \cup \{n\} = S(n)$.

Pro spor necht' $m \subset S(n) = n \cup \{n\}$, ale $m \not\subseteq n$. Potom musí být $n \in m$, tudíž podle Lemmatu 5.37 $n \subseteq m$, takže $n \cup \{n\} = S(n) \subseteq m$, což je spor s $m \subset S(n)$. \square

Lemma 5.43. Relace \in je lineární ostré uspořádání na ω . Neboli pro všechna $k, n, m \in \omega$ platí

- | | |
|---|-----------------------|
| 1. $n \notin n$, | ... antireflexibilita |
| 2. $m \in n \wedge n \in k \Rightarrow m \in k$, | ... tranzitivita |
| 3. $m \in n \vee m = n \vee n \in m$. | ... trichomie |

Důkaz. 1. Jak jsme dokázali v Lemmatu 5.37.

2. Podle předchozího lemmatu lze relaci \in zaměnit za \subset , což je tranzitivní. Šlo by to také přímo z vlastnosti $m \in n \Rightarrow m \subseteq n$, ale tohle je hezčí.

3. Pro pevně zvolené n to dokážeme indukcí podle m . Definujme množinu $X(n) := \{m \in \omega \mid m \in n \vee m = n \vee n \in m\}$. Dokážeme, že $X(n)$ je induktivní a tedy $X(n) = \omega$. Nejprve uvažme $n = 0$. Určitě $0 \in X(0)$, protože $0 = 0$. Indukční krok: je-li $m \in X(0)$, tak buď $m = 0$ nebo $0 \in m$. Každopádně $0 \in m \cup \{m\} = S(m)$ a tedy $S(m) \in X(0)$. Z toho také vyplývá, že $(\forall n \in \omega)(0 \in X(n))$. Nyní zvolme $n \neq 0$ a $m \in X(n)$.

- (a) $m \in n$, takže podle předchozího lemmatu $m \subset n$. Také $\{m\} \subseteq n$, tedy $S(m) \subseteq n$. Pokud $S(m) = n$ tak jsme hotoví. Pokud $S(m) \subset n$, tak podle předchozího lemmatu $S(m) \in n$.
- (b) $m = n$ nebo $n \in m$. Každopádně $n \in m \cup \{m\} = S(m)$.

Tedy $S(m) \in X(n)$ a $X(n) = \omega$. □

Věta 5.44. ω je dobře ostře uspořádaná relací \in .

Důkaz. Nechť $\emptyset \neq a \subseteq \omega$. Jelikož \in je lineární na ω , tak nám stačí najít minimální prvek a (bude automaticky i nejmenší). Zvolme nějaké $n \in a$. Pokud je minimální, tak jsme vyhráli. Jinak nechť $b := n \cap a$. Protože n je konečná, tak b je konečná (a neprázdná). Podle Lemma 5.14 má b minimální prvek, označme jej m . Tvrdíme, že m je minimální i v a . Kdyby existovalo nějaké $x \in a$ t.ž. $x \in m$ (je menší než m), tak dojdeme ke sporu. Jelikož $x \in m \in n$, tak $x \in n$ a máme $x \in b$. Ale m je minimální v b . □

Úmluva. Běžně to budeme zkracovat: pokud o nějaké množině prohlásíme, že je „dobře uspořádaná relací \in “, tak tím myslíme, že je „dobře ostře uspořádaná relací \in “.

Další věta nám umožní poznat, kdy je něco uspořádané stejně jako ω .

Věta 5.45 (o charakterizaci uspořádání \in na ω). *Nechť A je nekonečná množina s ostrým lineárním uspořádáním ' $<$ ' takovým, že pro každé $a \in A$ je množina $(\leftarrow, a]$ konečná. Potom je ' $<$ ' dobré ostré uspořádání a navíc jsou uspořádané množiny $(A, <)$ a (ω, \in) izomorfní.*

Důkaz. První část je téměř stejná jako důkaz poslední věty.

1. ' $<$ ' je dobré: Nechť $\emptyset \neq c \subseteq A$ a $a \in c$. Pokud a není minimální (nejmenší), tak označme $b := c \cap (\leftarrow, a]$. Platí $a \in b$, takže $\emptyset \neq b \subseteq (\leftarrow, a]$. Podle předpokladu je b konečná, takže má minimální prvek m . Chceme ukázat, že m je minimální i v c . Pro spor nechť existuje nějaké $x \in c$ t.ž. $x < m$. Ukážeme, že $x \in b$, což bude spor. Protože $x < m < a$, tak $x \in (\leftarrow, a]$ a navíc $x \in c$, takže $x \in b$.
2. $(A, <)$ a (ω, \in) jsou izomorfní: podle Věty 5.19 nastane jedna ze dvou možností:
 - (a) A je izomorfní s nějakou dolní množinou $B \subseteq \omega$. B není shora omezená, kdyby byla, tak $(\exists n)(\forall b \in B)(b \in n \vee b = n)$, takže $B \subseteq S(n)$, takže B by byla konečná, ale A je nekonečná, což je spor s $A \approx B$. Jelikož B není shora omezená, tak každé $n \in \omega$ je menší než nějaký prvek B a tedy $n \in B$, protože B je dolní množina. Tudíž $B = \omega$.
 - (b) ω je izomorfní s nějakou dolní množinou $C \subseteq A$. Opět C není omezená, stejným argumentem. A opět protože C je dolní množina, tak $C = A$. □

5.5 Různě velká nekonečna

Definice 5.46 (Spočetnost). Množina x je

- *spočetná*, pokud $x \approx \omega$,
- *nejvýše spočetná*, pokud je spočetná nebo konečná,
- *nespočetná*, pokud není nejvýše spočetná.

5.5.1 Spočetné množiny

Věta 5.47. *Platí*

1. *každá shora omezená podmnožina $A \subseteq \omega$ je konečná,*
2. *každá shora neomezená podmnožina $A \subseteq \omega$ je spočetná.*

Důkaz.

1. A je shora omezená $n \in \omega$, pak $A \subseteq S(n)$, tedy $\text{Fin}(A)$.
2. Je-li A konečná, tak má podle Lemmatu 5.14 maximální (největší) prvek vůči \in , tedy je omezená. Obměna: A neomezená $\Rightarrow A$ nekonečná. Potřebujeme ale spočetnost. Použijeme poslední větu. A je nekonečná, lineárně uspořádaná relací \in a pro každé n je $(\leftarrow, n] \subseteq S(n)$ konečná, tedy A a ω jsou izomorfní (vzhledem k \in), speciálně $A \approx \omega$. \square

Důsledek 5.48. *Množina x je nejvýše spočetná $\iff x \preceq \omega$.*

Důsledek 5.49. *Každá podmnožina spočetné množiny je nejvýše spočetná.*

Důkaz. Nechť je A spočetná, f bijekce mezi A a ω , $B \subseteq A$, potom $B \approx f[B] \subseteq \omega$, tedy $B \preceq \omega$. \square

Definice 5.50. Definujeme *lexikografické* (ostré) uspořádání $<_L$ na $\omega \times \omega$ jako

$$(m_1, n_1) <_L (m_2, n_2) \iff (m_1 \in m_2 \vee (m_1 = m_2 \wedge n_1 \in n_2))$$

Intuice. Lexikografické uspořádání je dobré na $\omega \times \omega$. Prvky jsou vlastně uspořádané do mřížky, sloupečky jsou nekonečné stoupající řetězce a n -tý sloupeček je menší než $(n+1)$ -ní sloupeček.

Příklad. Platí, že $\omega \times 2$ je izomorfní s ω — nekonečně sloupečků výšky dva. Ale $2 \times \omega$ není izomorfní s ω — dva nekonečné sloupečky. Všechno vůči \in .

Definice 5.51. Pro $m, n \in \omega$ definujeme $\max(m, n) := m$ pokud $n \in m$, jinak n . *Maximo-lexikografické* uspořádání na $\omega \times \omega$ definujeme jako

$$(m_1, n_1) <_{ML} (m_2, n_2) \iff \max(m_1, n_1) \in \max(m_2, n_2) \\ \vee (\max(m_1, n_1) = \max(m_2, n_2) \wedge (m_1, n_1) <_L (m_2, n_2))$$

Intuice. Procházíme jakoby čtverce/pravé úhly v nějaké vzdálenosti od počátku, a věci ve stejné vzdálenosti procházíme lexikograficky.

Úloha. Množina $(\omega \times \omega, <_{ML})$ je izomorfní s (ω, \in) , tedy $\omega \times \omega \approx \omega$. Stačí ověřit, že $(\omega \times \omega, <_{ML})$ splňuje všechny předpoklady té charakterizační věty. Tenhle důkaz je hezký tím, že nepotřebujeme aritmetiku.

Ukážeme, že vyrobit ze spočetných množin nespočetnou množinu není jenom tak. Podobně jako konečné sjednocení nebo konečný součin konečných množin je konečný.

Věta 5.52. *Jsou-li A, B spočetné množiny, pak $A \cup B$ a $A \times B$ jsou také spočetné.*

Důkaz. Máme bijekce $f : A \rightarrow \omega$ a $g : B \rightarrow \omega$. Definujeme zobrazení $h : A \cup B \rightarrow \omega \times 2$ jako

$$h(x) := \begin{cases} (f(x), 0), & \text{pro } x \in A, \\ (g(x), 1), & \text{jinak.} \end{cases}$$

Zobrazení h je prosté, ale nemusí to být bijekce. Takže $A \cup B \preceq \omega \times 2 \approx \omega$. Ale také $\omega \approx A \subseteq A \cup B$, takže $\omega \preceq A \cup B$ a podle Cantor-Bernsteinovy věty $A \cup B \approx \omega$.

Nyní pro $A \times B$. Definujeme $k : A \times B \rightarrow \omega \times \omega$ jako $k : (a, b) \mapsto (f(a), g(b))$. Protože je k bijekce, tak $A \times B \approx \omega \times \omega \approx \omega$. \square

Důsledek 5.53. *Konečná sjednocení a konečné součiny spočetných množin jsou spočetné (indukcí).*

Důsledek 5.54. *Množiny \mathbb{Z} a \mathbb{Q} jsou spočetné. V sekci 5.2 jsme to dokázali pomocí aritmetiky, ovšem teď to umíme i bez ní.*

Důsledek 5.55 (Dirichletův princip). *Je-li nespočetná množina sjednocením konečně mnoha množin, tak alespoň jedna z nich je nespočetná.*

Dobrá, co kdybychom dělali sjednocení, resp. součin spočetně mnoha spočetných množin? Tyto pojmy si formálně definujeme až v kapitole o axiomu výběru, zatím je můžeme vnímat intuitivně. Ukážeme, že součin bude nespočetný, nehledě na platnost axiomu výběru. Spočetnost sjednocení nelze v ZF rozhodnout, ale ukážeme, že v ZFC bude sjednocení spočetné.

5.5.2 Cantorova věta

Věta 5.56 (Cantorova). *Pro každou množinu x platí $x \prec \mathcal{P}(x)$.*

Důkaz. Zjevně $x \preceq \mathcal{P}(x)$, pomocí prostého zobrazení $f : x \rightarrow \mathcal{P}(x), a \mapsto \{a\}$. Pro spor předpokládejme, že existuje bijekce $f : x \rightarrow \mathcal{P}(x)$. Definujme množinu $T := \{a \in x \mid a \notin f(a)\}$. Nyní pro každé $a \in x$ nastane jedna ze dvou situací:

$$\begin{aligned} a \in T &\implies a \notin f(a) \implies T \neq f(a), \\ a \notin T &\implies a \in f(a) \implies T = f(a). \end{aligned}$$

V každém případě $T \neq f(a)$, takže T nemá vzor, což je spor s tím, že f je bijekce. \square

Důsledek 5.57. *Množina $\mathcal{P}(\omega)$ je nespočetná.*

Věta 5.58. *Univerzální třída V není množina.*

Důkaz. Kdyby byla, tak $V \prec \mathcal{P}(V)$. Ale určitě $\mathcal{P}(V) \preceq V$, což je spor. \square

Důsledek 5.59. *Pro každé $n \geq 1$ je třída všech n -prvkových množin vlastní třídou.*

Důkaz. Kdyby byla množinou, tak z axiomu sumy by byla její suma také množina. Ale její suma je V . \square

5.5.3 Kardinalita kontinua

Věta 5.60. ${}^\omega 2 \approx \mathcal{P}(\omega) \approx \mathbb{R} \approx [0, 1]$.

Důkaz. Podle Lemmatu 5.4 platí $\mathcal{P}(\omega) \approx {}^\omega 2$. Děláme charakteristické funkce posloupností: $\mathcal{P}(\omega) \rightarrow \{0, 1\}$. Jako další ukážeme $[0, 1] \approx {}^\omega 2$.

1. $[0, 1] \preceq {}^\omega 2$. Číslo $a \in [0, 1]$ zapíšeme binárně. Pokud $a = 0$, tak máme $0.000\dots$ a pokud $a > 0$, tak $0.a_0a_1a_2\dots$, kde nekonečně mnoho a_i je 1 abychom odstranili duplicity pro periodická čísla. Takže třeba $0.5_{10} = 0.1_2$ zapíšeme jako $0.0111\dots$. Tyto nekonečné posloupnosti jsou zjevně funkce z ω do $\{0, 1\}$.
2. ${}^\omega 2 \preceq [0, 1]$. Problém je, že posloupnosti $0.1000\dots$ a $0.0111\dots$ se zobrazí na stejné reálné číslo. Ale kdybychom to četli ve trojkové soustavě, tak už to budou různá čísla. Proto defingueme funkci $f : {}^\omega 2 \rightarrow [0, 1]$ jako

$$f : (a_0, a_1, a_2, \dots) \mapsto \sum_{i=0}^{\infty} \frac{a_i}{3^{i+1}}.$$

Tedy podle Cantor-Bernsteinovy věty $\mathcal{P}(\omega) \approx {}^\omega 2 \approx [0, 1]$. Zbývá ukázat $[0, 1] \approx \mathbb{R}$. Zřejmě $[0, 1] \preceq \mathbb{R}$, protože $[0, 1] \subseteq \mathbb{R}$. Opačně $\mathbb{R} \preceq [0, 1]$ například prostou funkcí

$$\arctan : \mathbb{R} \mapsto (-\pi/2, \pi/2),$$

kterou vhodně upravíme, aby obor hodnot byl podmnožinou intervalu $[0, 1]$. \square

Ukázali jsme, že reálných čísel je více než přirozených. Je přirozené položit si otázku, zda existuje něco mezi? Bylo by hezké, kdyby nejmenší množina, větší než přirozená čísla, byla reálná přímka (kontinuum). Tato myšlenka se nazývá hypotéza kontinua, anglicky Continuum hypothesis (CH). Formuloval ji už Cantor a říká, že neexistuje žádná množina x taková, že

$$\omega \prec x \prec \mathcal{P}(\omega) \approx \mathbb{R}.$$

Tedy každá nekonečná $x \subseteq \mathbb{R}$ je buď spočetná, nebo ekvivalentní s \mathbb{R} . Gödel (1940) dokázal, že CH nelze v ZFC vyvrátit. Cohen (1963) dokázal, že nelze v ZFC dokázat. Tedy je možné k ZFC bezesporně přidat jako axiom CH i \neg CH.

5.5.4 Algebraická čísla

Algebraická čísla jsou kořeny polynomů s celočíselnými koeficienty. Takže například $\sqrt{2}$ je algebraické číslo, protože je kořenem polynomu $x^2 - 2$. Čísla, která nejsou algebraická, nazýváme *transcendentní*.

Fakt 5.61. *Je-li A spočetná množina, potom*

1. *množina všech konečných podmnožin A je spočetná,*
2. *množina všech konečných posloupností prvků množiny A je spočetná.*

Tvrzení 5.62. *Algebraických čísel je spočetně mnoho.*

Důkaz. Polynom odpovídá nějaké konečné posloupnosti (a_0, a_1, \dots, a_n) celých čísel. Celých čísel je spočetně mnoho, takže těchto posloupností je také spočetně mnoho.

Tedy každému polynomu přiřadíme nějaké pořadové číslo. Navíc víme, že polynom stupně n má nejvýše n kořenů. Algebraických čísel je určitě alespoň spočetně mnoho, musíme ukázat, že jich není víc. Proto definujeme prosté zobrazení všech algebraických čísel do spočetné množiny $\omega \times \omega$. Každý reálný kořen x polynomu

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0, \quad a_0 \neq 0$$

je jednoznačně určen dvojicí (k, l) , kde k je číslo přiřazené posloupnosti koeficientů tohoto polynomu a l udává, že x je l -tý reálný kořen tohoto polynomu podle velikosti. Ovšem jednomu algebraickému číslu může odpovídat víc dvojic (k, l) , stačí rovnici vynásobit nějakou konstantou. Proto algebraickému číslu x přiřadíme ze všech dvojic (k, l) , které mu odpovídají, tu nejmenší vzhledem k maximo-lexikografickému uspořádání. \square

Důsledek 5.63. *Transcendentních čísel je nespočetně mnoho.*

6 Axiom výběru

Axiom výběru, anglicky Axiom of Choice (AC), má mnoho důležitých důsledků a je klíčový v mnoha oblastech matematiky, například v analýze a lineární algebře. Bez něj nelze dokázat spousta tvrzení, která by intuitivně měla platit. Jeho přidáním do Zermelova–Fraenkelovy teorie množin získáme teorii ZFC.

Nicméně axiom výběru je také kontroverzní, protože některé jeho důsledky odporují intuici, jako například princip dobrého uspořádání, který říká, že každou množinu lze dobře uspořádat. Nebo Banach-Tarski paradox, který uvádí postup, jak rozdělit kouli na konečný počet částí a tyto části přeskupit tak, aby vznikly dvě koule identické s tou původní.

6.1 Indexované soubory množin

Definice 6.1. *Soubor množin $\langle X_i \mid i \in I \rangle$ je zobrazení F s definičním oborem I , kde X_i označuje množinu $F(i)$. Říkáme, že I je *indexová třída* tohoto souboru a*

že x patří do souboru, jestliže pro nějaké $i \in I$ platí $x = X_i$. Definujeme

$$\begin{aligned}\bigcup_{i \in I} X_i &:= \bigcup \text{Rng}(F), \\ \bigcap_{i \in I} X_i &:= \bigcap \text{Rng}(F), \\ \prod_{i \in I} X_i &:= \{f \mid f : I \mapsto \bigcup_{i \in I} X_i \wedge (\forall i \in I)(f(i) \in X_i)\}.\end{aligned}$$

Definice kartézského součinu má smysl jen pro soubory indexované množinou, protože vlastní třídy nebudou nikam náležet.

Lemma 6.2. *Je-li I množina a $\langle X_i \mid i \in I \rangle$ soubor indexovaný I , potom jsou třídy $\bigcup_{i \in I} X_i$, $\bigcap_{i \in I} X_i$ a $\prod_{i \in I} X_i$ také množinami.*

Důkaz. $\text{Dom}(F) = I$ je množina, takže podle axiomu nahrazení je $\text{Rng}(F) = F[I]$ také množina. Proto jsou suma a průnik také množiny. Všimněme si, že produkt je podmnožinou množiny všech zobrazení z I do $\bigcup_{i \in I} X_i$, což je množina. \square

Pozorování 6.3. *Pokud pro každé $i \in I$ je $X_i = X$, tak $\prod_{i \in I} X_i = {}^I X$.*

Lemma 6.4. *Je-li $\langle X_i \mid i \in \omega \rangle$ spočetný soubor množin, kde na každém X_i existuje dobré uspořádání a $2 \preceq X_i$, potom je součin tohoto souboru nespočetný.*

Důkaz. Není těžké ukázat, že

$$\prod_{i \in \omega} 2 \preceq \prod_{i \in \omega} X_i.$$

Podle posledního pozorování ovšem platí $\prod_{i \in \omega} 2 = {}^\omega 2 \approx \mathcal{P}(\omega)$, což je podle Cantorovy věty nespočetná množina. \square

Důsledek 6.5. *Kartézský součin spočetně mnoha spočetných množin je nespočetný.*

6.2 Co axiom výběru tvrdí

Ukažme si motivaci za zavedením axiomu výběru. Mějme f , zobrazení množiny X na množinu Y a podívejme se na rozklad množiny X definovaný jako

$$r := \{f^{-1}[y] \mid y \in Y\}.$$

Existuje prosté zobrazení $g : Y \rightarrow X$?

- Pro konečné Y lze dokázat indukci. Neformálně si prostě konečně-mnohokrát vezmu nějaký prvek z $f^{-1}[y]$.
- Pro dobře uspořádané X vezmu z $f^{-1}[y]$ vždy ten nejmenší prvek.
- Obecně to v ZF dokázat nelze — museli bychom pro každé $y \in Y$ vybrat nějakého reprezentanta $x \in f^{-1}[y]$ z potenciálně nekonečné množiny, ale těch $y \in Y$ taky může být nekonečně mnoho.

Původní formulace axiomu výběru zněla následovně.

Princip 6.6 (Výběru). Pro rozklad r množiny X existuje *výběrová množina* $v \subseteq X$ taková, že $(\forall u \in r)(\exists x)(v \cap u = \{x\})$. Takže z každé rozkladové třídy vybereme jednoho reprezentanta.

Dnes se ovšem používá poněkud šikovnější formulace přes selektory.

Definice 6.7 (Selektor). Je-li R množina, pak funkci $f : R \rightarrow \bigcup R$ splňující

$$(\forall t \in R)(t \neq \emptyset \Rightarrow f(t) \in t),$$

nazýváme *selektor* na množině R . BÚNO můžeme předpokládat, že selektor je definovaný na množině $R \setminus \{\emptyset\}$ a pro každé $t \in \text{Dom}(f)$ platí $f(t) \in t$.

Axiom 6.8 (Výběru). Na každé množině existuje selektor.

Věta 6.9. *Tvrzení ekvivalentní s axiomem výběru:*¹

- *Princip dobrého uspořádání* — každou množinu lze dobře uspořádat.
- *Princip trichotomie* — relace \preceq je trichotomická.
- *Princip maximality*, také známý jako *Zornovo lemma*.

Trochu slabší důsledky:

- Každý vektorový prostor má bázi.
- Součin kompaktních prostorů je kompaktní.
- *Princip kompaktnosti z kombinatoriky*. Příklad použití: graf je 3-obarvitelný \Leftrightarrow každý jeho konečný podgraf je 3-obarvitelný.
- *Banach-Tarski paradox*.

Všechna tato tvrzení lze dokázat bez AC, pokud uvažujeme pouze konečné případy.

Lemma 6.10. *Následující tvrzení jsou ekvivalentní:*

1. *axiom výběru*,
2. *princip výběru*,
3. *pro každou množinovou relaci s existuje funkce $f \subseteq s$ t.ž. $\text{Dom}(f) = \text{Dom}(s)$,*
4. *kartézský součin neprázdného souboru neprázdných množin je neprázdný.*

Důkaz.

$1 \Rightarrow 2$ Nechť r je rozklad X , podle axiomu výběru existuje selektor f na r . Hledaná výběrová množina je $\text{Rng}(f)$.

¹“The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn’s lemma?” — Jerry Bona

2 \Rightarrow 3 Pokud $s = \emptyset$, potom $f = \emptyset$ a není co dokazovat. Proto nechť $s \neq \emptyset$. Definujeme rozklad r množiny s jako

$$r := \{ \{ (x, y) \in s \mid y \in \text{Rng}(s) \} \mid x \in \text{Dom}(s) \}.$$

Podle principu výběru existuje výběrová množina tohoto rozkladu, což je právě hledaná funkce f .

3 \Rightarrow 4 Neprázdný soubor neprázdných množin $\langle X_i \mid i \in I \rangle$ určuje relaci $s := \{ (i, x) \mid i \in I \wedge x \in X_i \}$. Podle 3 existuje funkce $f \subseteq s$ t.ž. $\text{Dom}(f) = \text{Dom}(s) = I$ a tedy f je prvkem uvažovaného produktu.

4 \Rightarrow 1 Nechť x je libovolná množina, musíme ukázat, že na ní existuje selektor. BÚNO předpokládejme, že $x \neq \emptyset$ a $\emptyset \notin x$. Identita na x určuje neprázdný soubor neprázdných množin $\langle y \mid y \in x \rangle$, který má podle 4 neprázdný kartézský součin. Všimněme si, že každý prvek tohoto součinu je selektorem na x . \square

Lemma 6.11. $AC \implies$ Sjednocení spočetného souboru (nejvýše) spočetných množin je (nejvýše) spočetné.

Důkaz. Uvažme soubor $\langle B_i \mid i \in I \rangle$, BÚNO $I = \omega$. Sestrojíme prosté zobrazení z $S := \bigcup_{i \in \omega} B_i$ do $\omega \times \omega$. Nechť E_i je množina všech prostých zobrazení $f : B_i \rightarrow \omega$, ze spočetnosti B_i je $E_i \neq \emptyset$, a definujeme soubor $\langle E_i \mid i \in \omega \rangle$. Podle posledního lemmatu je produkt tohoto souboru neprázdný, existuje tedy soubor $\langle f_i \mid i \in \omega \rangle$, kde $f_i \in E_i$. Definujeme $h : S \rightarrow \omega \times \omega$ jako $h : b \mapsto (i, f_i(b))$, kde i je nejmenší index z ω , že $b \in B_i$. \square

Poznámka. Bez AC lze bezesporně předpokládat, že nespočetná množina \mathbb{R} je sjednocením spočetně mnoha spočetných množin.

6.3 Princip maximality

Axiom výběru je ekvivalentní s řadou tvrzení, jedno z nejpoužívanějších je Zornovo lemma, také známé jako princip maximality. Důkaz ekvivalence vynecháme, ale nachází se ve skriptíčkách navazujícího předmětu, dostupných ZDE.

Definice 6.12 (Řetězec). Nechť (A, \leq) je uspořádaná množina. Podmnožinu $B \subseteq A$ nazveme *řetězcem* v A , je-li B lineárně uspořádaná relací \leq .

Princip 6.13 (Maximality (PM)). Nechť (A, \leq) je uspořádaná množina, kde každý řetězec je shora omezený. Potom pro každé $a \in A$ existuje maximální prvek b množiny A takový, že $a \leq b$.

Poznámka. Často se používá pro uspořádání $(A \subseteq, \subseteq)$, kde $A \subseteq \mathcal{P}(x)$. Pak pro řetězec $B \subseteq A$ stačí ukázat, že $\bigcup B \in A$. $\bigcup B \in A$ je totiž horní mez B vzhledem k \subseteq .

Princip 6.14 (Maximality II (PMS)). Nechť (A, \leq) je uspořádaná množina, kde každý řetězec má supremum. Potom pro každé $a \in A$ existuje maximální prvek b množiny A takový, že $a \leq b$.

Úloha. Dokažte $(PM) \iff (PMS)$.

Přechodem k inverznímu uspořádání dostáváme z principu maximality princip minimality.

Princip 6.15 (Minimality). Nechť (A, \leq) je uspořádaná množina, kde každý řetězec je zdola omezený. Potom pro každé $a \in A$ existuje minimální prvek b množiny A takový, že $b \leq a$.

6.4 Princip trichotomie

Princip 6.16 (Trichotomie). Pro libovolné množiny x, y platí $x \preceq y$ nebo $y \preceq x$.

Věta 6.17. *Princip maximality \implies princip trichotomie.*

Důkaz. Nejprve si připomeňme, že inverzní zobrazení k prostému zobrazení je prosté. Nyní nechť x, y jsou množiny, chceme sestavit prosté zobrazení x do y , nebo y do x . Definujme množinu

$$P := \{f \mid f \text{ je prosté zobrazení} \wedge \text{Dom}(f) \subseteq x \wedge \text{Rng}(f) \subseteq y\}.$$

Všimněme si, že uspořádaná množina (P, \subseteq) splňuje podmínky principu maximality, jelikož sjednocení řetězce prostých zobrazení je prosté zobrazení. Nechť g je nějaký maximální prvek P . Kdyby obě množiny $x \setminus \text{Dom}(g)$ a $y \setminus \text{Rng}(g)$ byly neprázdné, tak by g šlo rozšířit o další dvojici, což je spor s maximalitou g . Proto buď $\text{Dom}(g) = x$ a potom $x \preceq y$, nebo $\text{Rng}(g) = y$ a potom $y \preceq x$. \square

Tvrzení 6.18. $AC \implies \omega$ je nejmenší nekonečná množina.

Důkaz. Je-li x spočetná, tak $\omega \approx x$. Je-li nespočetná, tak z trichotomie buď $\omega \preceq x$ nebo $x \preceq \omega$. Jelikož x není spočetná ani konečná, tak druhá varianta nenastane. \square

Důsledek 6.19. *Množina x je konečná \iff je dedekindovsky konečná.*

Důkaz. V ZF jsme dokázali, že každá konečná množina je ded. konečná. Z toho obměnou, že každá ded. nekonečná je nekonečná. Nyní ukážeme, že každá nekonečná je ded. nekonečná. Z předchozího lemma víme, že pokud je x nekonečná, tak $\omega \preceq x$ z Lemmatu 5.41, že ω je ded. nekonečná. Není těžké ukázat, že x musí být také ded. nekonečná. \square

6.5 Princip dobrého uspořádání

Princip 6.20 (Dobrého uspořádání (WO)). Každou množinu lze dobře uspořádat.

Věta 6.21. *Well-ordering principle \implies axiom výběru*

Důkaz. Nechť x je množina splňující $x \neq \emptyset$ a $\emptyset \notin x$. Chceme sestavit selektor $f : x \rightarrow \bigcup x$. Ten musí splnit $(\forall y \in x) : f(y) \in y$. Podle WO existuje dobré uspořádání \leq na $\bigcup x$ a každá $y \in x$ je neprázdna podmnožina $\bigcup x$, tedy má nejmenší prvek vůči \leq . Selektor f definujeme jako $f : y \mapsto \min_{\leq}(y)$. \square

Úloha. Dokažte $(PM) \implies (WO)$.

7 Ordinální čísla

Ordinální čísla jsou zobecnění přirozených čísel a udávají typy dobře uspořádaných množin. Pomocí ordinálních čísel pak lze nadefinovat kardinální čísla, což jsou speciální ordinální čísla, která měří mohutnosti množin. Ordinální čísla definujeme tak, aby byla dobře uspořádána relací \in , takže na nich budeme moci provádět takzvanou transfinitní indukci.

7.1 Tranzitivní třídy

Definice 7.1. Třída X je *tranzitivní*, pokud $y \in x \in X \Rightarrow y \in X$.

Pozorování 7.2. *Ekvivalentně: $x \in X \Rightarrow x \subseteq X$.*

Pozorování 7.3. X je tranzitivní $\iff \bigcup X \subseteq X$.

Lemma 7.4. *Vlastnosti tranzitivních tříd.*

1. Jsou-li X, Y tranzitivní třídy, pak $X \cap Y$ a $X \cup Y$ jsou také tranzitivní.
2. Jsou-li všechny prvky $x \in X$ třídy X tranzitivní, tak $\bigcap X$ a $\bigcup X$ jsou také tranzitivní.
3. Je-li X tranzitivní třída a relace \in je tranzitivní na X , tak každé $x \in X$ je tranzitivní množina.
4. Je-li každé $x \in X$ tranzitivní množina, pak je relace \in tranzitivní na X .

Důkaz.

1. Plyne přímo z definice.
2. Ukážeme pro průnik, suma podobně. Necht' $y \in z \in \bigcap X$, chceme ukázat $y \in \bigcap X$. Protože je každá $x \in X$ tranzitivní, tak z $y \in z \in x$ máme $y \in x$, tedy $y \in \bigcap X$ a X je tranzitivní.
3. Je-li \in tranzitivní na X a $z \in y \in x \in X$, tak $z \in x$, tedy x je tranzitivní množina.
4. Je-li $x, y, z \in X$ a $x \in y \in z$, tak z tranzitivity z je $x \in z$, tedy relace \in je tranzitivní na X . \square

7.2 Uspořádání ordinálních čísel relací náležení

Definice 7.5. Množina x je *ordinální číslo*, pokud

1. x je tranzitivní, a
2. relace \in je dobré ostré uspořádání na x .

Třidu všech ordinálních čísel značíme On

Poznámka. Každé $n \in \omega$ i samotné ω jsou ordinální čísla.

Lemma 7.6. *Třída On je tranzitivní.*

Důkaz. Ukážeme, že každé $y \in x \in \text{On}$ je také ordinální číslo, tedy $y \in \text{On}$. Protože x je ordinál, tak relace \in je na x dobré uspořádání, speciálně je tedy tranzitivní. Podle třetí části Lemmatu 7.4 je potom $y \in x$ tranzitivní množina. Ještě musíme ukázat, že \in je dobré uspořádání na y . Ale to je, jelikož $y \in x \Rightarrow y \subseteq x$ a relace „být dobré uspořádání“ je dědičná (x je dobře uspořádaná, protože to je ordinál). \square

Lemma 7.7. *Relace \in je tranzitivní na On .*

Důkaz. Ukázali jsme, že On je tranzitivní a navíc každé $x \in \text{On}$ je tranzitivní, takže podle čtvrté části Lemmatu 7.4 je relace \in tranzitivní na On . \square

Lemma 7.8. *Pro každá dvě $x, y \in \text{On}$ platí*

1. $x \notin x$,
2. $x \cap y \in \text{On}$,
3. $x \in y \iff x \subset y$.

Důkaz.

1. Z antireflexivity \in na x .
2. Podle Lemmatu 7.4 je $x \cap y$ tranzitivní množina a je dobře uspořádaná relací \in , protože to je podmnožinou ordinálu x .
3. Směr ' \Rightarrow ' z tranzitivity y a 1. Pro opačný směr nechť $x \subset y$. Protože y je dobře uspořádaná, tak $\emptyset \neq y \setminus x \subseteq y$ má nejmenší prvek vůči \in , označme jej z . Ukážeme, že $z = x$. Nejprve inkluze $x \subseteq z$. Nechť $u \in x$, protože $x \subseteq y$, tak $u \in y$. Protože y je ordinál, tak \in je lineární na y , tedy u můžeme porovnat se z . Jsou tři možnosti
 - (a) $u \in z$, to jsme chtěli,
 - (b) $u = z$, ale $z \notin x$, takže $u \notin x$, což je spor,
 - (c) $z \in u$, z tranzitivity x máme $z \in u \in x \implies z \in x$, což je opět spor.

Nyní inkluze $z \subseteq x$. Nechť $u \in z$, podle tranzitivity y máme $u \in z \in y \implies u \in y$, ukážeme $u \in x$. Kdyby $u \notin x$, tak u je menší prvek v doplňku $y \setminus x$ než z , což je spor s minimalitou z . \square

Věta 7.9. *Relace \in je dobré (ostré) uspořádání na On .*

Důkaz. Je tranzitivní a antireflexivní, takže to je ostré uspořádání.

1. Trichotomie (a z toho linearita). Nechť $x, y \in \text{On}$, chceme je porovnat. Podívejme se na množinu $z := x \cap y \in \text{On}$. Ukážeme, že $z = x$ nebo $z = y$. Kdyby $z \subset x$ a $z \subset y$, pak podle minulého lemmatu $z \in x$ a $z \in y$, čili $z \in z$, což je spor. Nyní rozbor případů:
 - (a) $x = y$, pak jsme skončili,
 - (b) $z = x \wedge z \subset y$, pak $x \in y \dots$ podle předchozího lemmatu,
 - (c) $z = y \wedge z \subset x$, pak $y \in x \dots$ podle předchozího lemmatu.

2. Dobrost dokážeme podobně jako pro ω . Nechť $A \subseteq \text{On}$ je neprázdná a $\alpha \in A$. Není-li α minimální, označme $b := \alpha \cap A$. BÚNO $b \neq \emptyset$, jinak by bylo minimální. Jelikož $b \subseteq \alpha$ a α je ordinální číslo, tak je b dobře uspořádané a má nejmenší prvek β (vůči \in). Tvrdíme, že β je minimální v A . Kdyby ne, tak existuje nějaké $\gamma \in \beta$ t.ž. $\gamma \in A$. Ale $\beta \in \alpha$, takže z tranzitivity α je $\gamma \in \alpha$. Tedy $\gamma \in b$, což je spor s minimalitou β . \square

Důsledek 7.10. *Třída On není množina.*

Důkaz. Ukázali jsme, že On je tranzitivní a \in je na ní dobré ostré uspořádání, tedy kdyby to byla množina, tak je to ordinál, tedy $\text{On} \in \text{On}$, což je spor. \square

Důsledek 7.11. *Je-li X tranzitivní vlastní třída dobře uspořádaná relací \in , pak $X = \text{On}$.*

Důkaz. Jelikož je X tranzitivní, tak pokud $x \in X$, potom $x \subseteq X$. Protože X je dobře uspořádaná relací \in , tak z dědičnosti je x také dobře uspořádaná. Navíc jelikož je \in tranzitivní na X , tak x je tranzitivní množina. Proto je x ordinální číslo, čili $X \subseteq \text{On}$. Pro spor nechť platí pouze ostrá inkluze a $x \in \text{On} \setminus X$. Ukážeme, že $X \subseteq x$, což je spor s tím, že X je vlastní třída.

Nechť $y \in X$, kdyby $y \notin x$, tak z trichomie \in na On musí být $x \in y$. Z tranzitivity X bychom pak měli $x \in X$, což je spor. \square

7.3 Vlastnosti ordinálních čísel

Úmluva. Ordinální čísla značíme řeckými písmeny α, β, γ , píšeme $\alpha < \beta$ namísto $\alpha \in \beta$ a $\alpha \leq \beta$ namísto $\alpha \in \beta \vee \alpha = \beta$.

Lemma 7.12. *Pro ordinální čísla platí následující.*

1. Nechť $x \subseteq \text{On}$ je množina. Pak x je ordinální číslo $\iff x$ je tranzitivní.
2. Nechť $\emptyset \neq A \subseteq \text{On}$ je třída. Pak $\bigcap A$ je nejmenší prvek A (vzhledem k $<$).
3. Nechť $A \subseteq \text{On}$ je množina, pak $\bigcup A$ je ordinální číslo a dokonce to je supremum A .

Důkaz.

1. Směr ' \Rightarrow ' z definice. Pro opačný směr nechť x je tranzitivní, potřebujeme aby \in bylo dobré uspořádání na x . Ale podle předchozí věty je \in dobré uspořádání na On , takže z dědičnosti i na $x \subseteq \text{On}$.
2. Podle předchozí věty má A nejmenší prvek α , ukážeme $\alpha = \bigcap A$. Pro libovolné $\beta \in A$ platí $\alpha \leq \beta$. Buď $\beta = \alpha$ nebo $\alpha \in \beta$, protože ordinály jsou tranzitivní, tak $\alpha \subseteq \beta$. Každopádně $\alpha \subseteq \beta$, proto $\alpha = \bigcap A$.
3. Podle Lemmatu 7.4 je $\bigcup A$ tranzitivní, protože všechny prvky A jsou tranzitivní. Jelikož to je tranzitivní množina ordinálních čísel, tak podle 1 je to ordinál. Teď ještě musíme ukázat, že to je supremum A . Nejprve, že to je horní mez. Nechť $\alpha \in A$, potom $\alpha \subseteq \bigcup A =: \beta$. Pokud $\alpha = \beta$, tak jsme skončili. Pokud $\alpha \subset \beta$, tak podle Lemmatu 7.8 je $\alpha \in \beta$. Každopádně $\alpha \leq \beta$, tedy β je horní mez množiny A . Nyní ukážeme, že žádné $\gamma < \beta$ horní mez být nemůže. Pokud $\gamma < \beta$, neboli $\gamma \in \bigcup A$, tak existují $\alpha \in A$ t.ž. $\gamma \in \alpha$, neboli $\gamma < \alpha$, tedy γ není horní mezí A . \square

Důsledek 7.13. *Ordinál ω je supremum množiny všech přirozených čísel v On . To znamená, že ω je nejmenší nekonečné ordinální číslo. Konečné ordinály jsou právě přirozená čísla.*

Důkaz. Podle lemma je $\sup(\omega) = \bigcup \omega$ a není těžké ukázat, že $\bigcup \omega = \omega$. Je-li x nekonečné ordinální číslo, tak $\omega \preceq x$, jak jsme dokázali v kapitole o AC. Je-li x konečné, tak z trichotomie nastane jeden ze tří případů:

1. $x < \omega$, neboli $x \in \omega$, tedy x je přirozené číslo,
2. $x = \omega$, ale to je spor s konečností x ,
3. $x > \omega$, neboli $\omega \in x$, ale protože x je ordinál, tak je tranzitivní, tedy $\omega \subseteq x$, což je spor s konečností x . \square

7.4 Typy dobře uspořádaných množin

Jsou-li dvě množinové relace izomorfní, tak se podstatně neliší, přestože popisují vztahy mezi prvky různých množin. Dává proto smysl uvažovat ekvivalenci „být izomorfní“ na třídě všech relací. Je snadné nahlédnout, že ekvivalenční třídy této relace jsou vlastní třídy, proto nemůžeme udělat rozklad. Ale bylo by hezké, kdybychom mohli pro každou ekvivalenční třídu sestavit nějakého reprezentanta, abychom pak mohli vše týkající se relací daného typu dokazovat na tomto reprezentantovi. Tito reprezentanti jsou právě ordinální čísla.

Věta 7.14 (O typu dobrého uspořádání). *Je-li a množina dobře uspořádaná relací R , pak existuje právě jedno ordinální číslo α a jednoznačně určený izomorfismus (a, \leq_R) a $(\alpha, <)$. Ordinálnímu číslu α říkáme typ uspořádané množiny (a, \leq_R) .*

Poznámka. Tohle byla původní Cantorova definice ordinálních čísel. Ta naše je Von-Neumannova.

Důkaz vynecháme, ale je možné ho najít ve skriptíčkách navazujícího předmětu, dostupných ZDE.

7.5 Princip transfinitní indukce

Lemma 7.15. *Pokud $\alpha \in \text{On}$, pak $\alpha \cup \{\alpha\}$ je nejmenší ordinální číslo větší než α .*

Důkaz. Nejprve ukážeme, že to je ordinální číslo. Protože je α tranzitivní, tak $\alpha \cup \{\alpha\}$ je taky tranzitivní (rozbor případů). Protože $\alpha \subseteq \text{On}$, tak dokonce je $\alpha \cup \{\alpha\}$ tranzitivní množina ordinálních čísel, podle posledního lemmatu je tedy také ordinálním číslem. Nyní, že je nejmenší. Je-li $\beta < \alpha \cup \{\alpha\}$, neboli $\beta \in \alpha \cup \{\alpha\}$, pak $\beta \in \alpha$ nebo $\beta = \alpha$, tedy $\beta \leq \alpha$. \square

Definice 7.16. Je-li α ordinální číslo, tak ordinál $\alpha + 1 := \alpha \cup \{\alpha\}$ nazýváme *následníkem* α , a ordinál α nazýváme *předchůdcem* $\alpha + 1$.

Definice 7.17. Ordinální číslo α je *izolované*, pokud $\alpha = 0$ nebo α má předchůdce. Jinak je α *limitní*.

Příklad. Každé $n \in \omega$ nebo $\omega + 1 = \omega \cup \{\omega\}$ jsou izolované, ale ω je limitní.

Věta 7.18 (Princip transfinite indukce). *Je-li $A \subseteq \text{On}$ třída t.ž. pro $\forall \alpha \in \text{On}$ platí*

$$\alpha \subseteq A \Rightarrow \alpha \in A,$$

potom $A = \text{On}$.

Důkaz. Pro spor nechť $\text{On} \setminus A$ není prázdná. Jelikož (On, \leq) je dobře uspořádaná množina, tak existuje nejmenší prvek α této třídy. Protože α je nejmenší, tak každé $\beta \in \alpha$ musí být prvkem A . Tedy $\alpha \subseteq A$ a z předpokladu $\alpha \in A$, což je spor. \square

Ekvivalentně lze princip transfinite indukce formulovat zvlášť pro izolované a limitní ordinály. S touto formulací se pak lépe dokazují některá tvrzení.

Věta 7.19 (Princip transfinite indukce II). *Je-li $A \subseteq \text{On}$ třída splňující*

1. $0 \in A$,
2. $\alpha \in A \Rightarrow \alpha + 1 \in A$, *... tohle je přesně indukce pro přirozená čísla*
3. *je-li α limitní, pak $\alpha \subseteq A \Rightarrow \alpha \in A$,*

potom $A = \text{On}$.

Pomocí transfinite indukce dokazujeme vlastnosti různých nekonečných objektů. Transfinite rekurze nám zase umožňuje konstruovat různé rekurzivně definované nekonečné objekty.

Věta 7.20 (O konstrukci transfinite rekurzí). *Je-li $G : V \rightarrow V$ třídivé zobrazení, pak existuje právě jedno třídivé zobrazení $F : \text{On} \rightarrow V$ splňující*

$$F(\alpha) = G(F[\alpha]).$$

Můžeme použít i jinou konstrukci, třeba $F(\alpha) = G(F \upharpoonright \alpha)$. Zkrátka něco rekurentního.

Intuice. $F(0) = G(0)$, $F(1) = G(F[1]) = G(\{F[0]\})$, prostě už to mám pro všechna menší ordinální čísla a pomocí toho udělám to další. Umožňuje konstrukci funkcí definovaných rekurzivně. Například můžeme definovat $F_n(0) := n$ a $F_n(S(m)) := S(F_n(m))$.

Věta 7.21. *Axiom výběru \implies princip dobrého uspořádání.*

Nástin důkazu. Nechť A je množina, a g selektor na $\mathcal{P}(A)$. Pomocí transfinite rekurze sestojíme dobré uspořádání množiny A . Definujeme funkci $f(0) := g(A)$, $f(\beta) := g(A \setminus f[\beta])$, takže pro β si z A vyberu nějaký prvek, který jsem ještě nepoužil. Vlastně si prvky té množiny A očíslovujeme, jako by to byla ordinální čísla. \square

7.6 Aplikace konstrukce transfinite rekurze

Nejprve dva příklady, na které rekurze není potřeba.

Úloha. \mathbb{R}^3 je sjednocením navzájem mimoběžných přímk.

Úloha. \mathbb{R}^3 je sjednocením navzájem disjunktních kružnic.

Tohle už bez rekurze nejde, nebo na to alespoň zatím nikdo nepřišel.

Úloha. V \mathbb{R}^2 existuje množina, která má s každou přímkou společné právě dva body. Hyperbola je k tomu docela blízko, ale ne úplně.

Úloha. \mathbb{R}^3 je sjednocením navzájem disjunktních jednotkových kružnic.

Řešení. Pomocí AC, WO a transfinite rekurze. Očíslujeme body \mathbb{R}^3 ordinálními čísly a dobře je uspořádáme jako $x_0, x_1, \dots, x_\omega, x_{\omega+1}, \dots$, potom

$$\mathbb{R}^3 = \{x_\alpha \mid \alpha < 2^\omega\},$$

kde 2^ω je kardinální číslo t.ž. $2^\omega \approx \mathcal{P}(\omega) \approx \mathbb{R}$, t.j. nejmenší ordinální číslo s touto mohutností. Obecně když jsou κ, α kardinální čísla, tak $\alpha < \kappa \Rightarrow \alpha \prec \kappa$.

Vyrobíme soubor $\langle C_\alpha \mid \alpha < 2^\omega \rangle$ disjunktních jednotkových kružnic (nebo \emptyset , když ji nepotřebuji) tak, aby $\bigcup_{\alpha < 2^\omega} C_\alpha = \mathbb{R}^3$. Stačí definovat C_α rekurzivně, známe-li $\{C_\beta \mid \beta < \alpha\}$. Pomocí C_α chci pokrýt bod x_α , pokud $x \in \bigcup_{\beta < \alpha} C_\beta$, potom $C_\alpha := \emptyset$ (bod jsem již pokryl). Jinak C_β leží v méně než 2^ω nadrovinách (nejhorší případ: každá kružnice v jedné). Tedy existuje nadrovina H_α procházející x_α neobsahující žádnou kružnici $C_\beta, \beta < \alpha$. Kružnice ji ale mohou protínat ovšem vždy nejvýše ve dvou bodech, opět v nejhorším případě dva průsečíky, tedy množina průsečíků $\bigcup_{\beta < \alpha} (H_\alpha \cap C_\beta) \preceq 2 \times \alpha \prec 2^\alpha$. Chceme najít nějakou kružnici co leží v rovině H_α ale neprotíná žádný z těch průsečíků. Každý bod $x \in H_\alpha$ určuje nejvýše 2 jednotkové kružnice procházející body x_α a x . Tedy počet zakázaných kružnic je maximálně $4 \times \alpha \prec 2^\omega$. Čili lze zvolit (pomocí AC) C_α tak, že $x_\alpha \in C_\alpha$, $C_\alpha \subseteq H_\alpha$ a $C_\beta \cap C_\alpha = \emptyset$ pro $\beta < \alpha$. Použijeme selektor na $\mathcal{P}(\{C \mid C \text{ je jednotková kružnice v } \mathbb{R}^3\})$. Nakonec

$$\bigcup_{\alpha < 2^\omega} C_\alpha = \{x_\alpha \mid \alpha < 2^\omega\} = \mathbb{R}^3.$$

Zdroje

Tento text jsou převážně mé poznámky z předmětu NAIL063, vyučovaného na MFF UK doc. Kynčlem, web přednášky ZDE. Přednáška vychází z první a části druhé kapitoly [1]. Velmi hezké povídání o úvodu do teorie množin je také na webu matematického korespondenčního semináře [3]. V kapitole o logice jsem vycházel ze skript doktora Bulína [2]. Některé z vynechaných důkazů ze sekce o axiomu výběru a o ordinálních číslech jsou ve skriptíčkách navazujícího předmětu [4].

Pokud jste v textu našli nějaký překlep nebo chybu, ať už stylistickou či matematickou, tak mě prosím kontaktujte na smolikj@matfyz.cz.

- [1] Bohuslav Balcar a Petr Štěpánek. *Teorie množin*. Vydání 2., opravené a rozšířené. Praha: Academia, 2001. ISBN: 80-200-0470-X.
- [2] Jakub Bulín. *NAIL062 Výroková a predikátová logika: zápisky z přednášky*. 2023, s. 71–82. URL: <https://github.com/jbulin-mff-uk/nail062/raw/main/lecture/lecture-notes/lecture-notes.pdf> (cit. 10.12.2023).
- [3] Matematický korespondenční seminář. *Do nekonečna a ještě dál*. URL: <https://prase.cz/archive/35/serial.pdf> (cit. 25.12.2023).
- [4] Jakub Smolík. *Infinite Sets*. URL: https://raw.githubusercontent.com/Couleslaw/my-papers/main/en/Infinite_sets.pdf.